PATENT OFFICE
JAPANESE COVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: November 5, 1998
Application Number : P10-315172
Applicant(s) : Nippon Telegraph & Telephone Corporation

February 5, 1999

Commissioner,
Patent Office Takeshi ISAYAMA

Number of Certificate: H 11-3003899

09/277417

4-90

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１１月 ５日

出 願 番 号
Application Number: 平成１０年特許願第３１５１７２号

出 願 人
Applicant (s): 日本電信電話株式会社

１９９９年 ２月 ５日

特 許 庁 長 官
Commissioner,
Patent Office 保佐山建志

出証番号 出証特平１１－３００３８９９

【書類名】　特許願

【整理番号】　NTTH106186

【提出日】　平成10年11月 5日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/28

【発明の名称】　接続制御方法および通信網と接続制御プログラムおよびデータ構造を記録した記録媒体

【請求項の数】　64

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　久田　裕介

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　小野　諭

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　市川　晴久

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代表者】　宮津　純一郎

【代理人】

【識別番号】　100083806

【弁理士】

【氏名又は名称】　三好　秀和

【電話番号】　03-3504-3075

【選任した代理人】

【識別番号】　100068342

【弁理士】

【氏名又は名称】　三好　保男

【先の出願に基づく優先権主張】

【出願番号】　平成10年特許願第 79837号

【出願日】　平成10年 3月26日

【先の出願に基づく優先権主張】

【出願番号】　平成10年特許願第171930号

【出願日】　平成10年 6月18日

【先の出願に基づく優先権主張】

【出願番号】　平成10年特許願第224861号

【出願日】　平成10年 8月 7日

【手数料の表示】

【予納台帳番号】　001982

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701396

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　接続制御方法および通信網と接続制御プログラムおよびデータ構造を記録した記録媒体

【特許請求の範囲】

【請求項１】　通信網におけるユーザ個人を隠蔽した通信の接続制御方法であって、

第１の機関がユーザの特性を識別する第１の機関の付与情報をユーザに付与し、

第２の機関が前記第１の機関の付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定し、

第３の機関がアクセス権を示す個別化アクセスチケットを発行し、

第４の機関が発信者からの発信要求に対して前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うこと

を特徴とする接続制御方法。

【請求項２】　前記第１の機関の付与情報が役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含む１対１個別化アクセスチケットであり、

第４の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを特徴とする請求項１記載の接続制御方法。

【請求項３】　前記第１の機関の付与情報が発信者役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が発信者役割識別

出証特平１１－３００３８９９

子と１個以上の着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含む１対Ｎ個別化アクセスチケットであり、

第４の機関は発信者からの接続要求を、前記発信者役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを特徴とする請求項１記載の接続制御方法。

【請求項４】　前記個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストにそのチケットを登録している場合は、第４の機関は当該接続要求を拒否することを特徴とする請求項１または２または３記載の接続制御方法。

【請求項５】　アクセス権を示す情報である個別化アクセスチケットを用いて、ユーザ間の通信を制御する接続制御方法であって、

前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを特徴とする接続制御方法。

【請求項６】　前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、

個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項５記載の接続制御方法。

【請求項７】　前記個別化アクセスチケットが発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含み、

第４の機関が発信者からの接続要求に対して、発信者役割識別子、１個以上の着信者役割識別子、個別化アクセスチケット、および個別化アクセスチケットに

対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項５記載の接続制御方法。

【請求項８】　前記検証結果が正しくても、個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを特徴とする請求項５記載の接続制御方法。

【請求項９】　個別化アクセスチケット変更権(Enabler）により第３の機関において所有者を変更するときの接続制御方法であって、

第１の個別化アクセスチケットの所有者役割識別子を第１の個別化アクセスチケット変更権(Enabler）で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler）および第１の役割識別子により新たな所有者役割識別子を変更し、第３の個別化アクセスチケットを作成することを特徴とする接続制御方法。

【請求項１０】　個別化アクセスチケット変更権(Enabler）により第３の機関において会員を追加するときの接続制御方法であって、

所有者が同一である複数の第４の個別化アクセスチケットの所有者役割識別子をそれぞれ第３の個別化アクセスチケット変更権(Enabler）と照合し、正しい場合に、前記第３の個別化アクセスチケット変更権を用いて、前記所有者役割識別子と前記すべての第４の個別化アクセスチケットのすべての会員役割識別子から構成される第５の個別化アクセスチケットを作成することを特徴とする接続制御方法。

【請求項１１】　個別化アクセスチケット変更権(Enabler）により第３の機関において会員を分割するときの接続制御方法であって、

第６の個別化アクセスチケットの所有者役割識別子を第４の個別化アクセスチケット変更権(Enabler）と照合し、正しい場合に、前記第４の個別化アクセスチケット変更権を用いて、前記所有者役割識別子と前記第６の個別化アクセスチケットの一部の会員役割識別子から構成される第７の個別化アクセスチケットを複

数作成することを特徴とする接続制御方法。

【請求項１２】　個別化アクセスチケット変更権(Enabler) により第３の機関において個別化アクセスチケットを新規生成するときの接続制御方法であって、

新規生成する個別化アクセスチケットの所有者役割識別子とする役割識別子と、会員役割識別子とするすべての第５の役割識別子について、それぞれの役割識別子の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第４の役割識別子を所有者役割識別子とする個別化アクセスチケットを新規生成することを特徴とする接続制御方法。

【請求項１３】　通信網においてユーザ個人を隠蔽した通信を制御可能とする通信網であって、

ユーザの特性を識別する付与情報をユーザに付与する第１の機関と、

前記付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定する第２の機関と、

アクセス権を示す個別化アクセスチケットを発行する第３の機関と、

発信者からの発信要求に対して前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う第４の機関と

を有することを特徴とする通信網。

【請求項１４】　前記第１の機関の付与情報が役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、

前記第４の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換

することで接続制御を行う手段を有することを特徴とする請求項１３記載の通信網。

【請求項１５】　前記第１の機関の付与情報が発信者役割識別子と個別化アクセスチケット変更権(Enabler）であり、前記発信者の指定情報が発信者役割識別子と１個以上の着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含み、

第４の機関は発信者からの接続要求を、前記発信者役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを特徴とする請求項１３記載の通信網。

【請求項１６】　前記第４の機関は、前記個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストに該個別化アクセスチケットを登録している場合は、第４の機関は当該接続要求を拒否する拒否手段を有することを特徴とする請求項１３または１４または１５記載の通信網。

【請求項１７】　アクセス権を示す情報である個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法を実施するプログラムを記録した記録媒体であって、

前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項１８】　前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、

個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化

アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項１７記載の接続制御プログラムを記録した記録媒体。

【請求項１９】　前記個別化アクセスチケットが発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含み、

第４の機関が発信者からの接続要求を、発信者役割識別子、１個以上の着信者役割識別子、個別化アクセスチケット、および個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項１７記載の接続制御プログラムを記録した記録媒体。

【請求項２０】　前記検証結果が正しくても、個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを特徴とする請求項１７記載の接続制御プログラムを記録した記録媒体。

【請求項２１】　個別化アクセスチケット変更権(Enabler) により第３の機関において所有者を変更する方法を実施するプログラムを記録した記録媒体であって、

第１の個別化アクセスチケットの発信者役割識別子を第１の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler) および第１の役割識別子により新たに発信者役割識別子を変更し、第３の個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項２２】　個別化アクセスチケット変更権(Enabler) により第３の機関において会員を追加する方法を実施するプログラムを記録した記録媒体であって、

第４の個別化アクセスチケットの発信者役割識別子を第３の個別化アクセスチ

ケット変更権(Enabler) と照合し、正しい場合に、１個以上の第４の個別化アクセスチケット変更権(Enabler) 、１個以上の第２の役割識別子により１個以上の新たな着信者役割識別子に追加し、第５の個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項２３】　個別化アクセスチケット変更権(Enabler) により第３の機関において会員を削除する方法を実施するプログラムを記録した記録媒体であって、

第６の個別化アクセスチケットの発信者役割識別子を第４の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、１個以上の第５の個別化アクセスチケット変更権(Enabler) 、１個以上の第３の役割識別子により１個以上の着信者役割識別子を削除し、第７の個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項２４】　個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

個別化アクセスチケットは、発信者フラグ、移転制御フラグ、発信者役割識別子、着信者役割識別子、有効期限、および第３の機関の秘密鍵による署名から構成され、

役割識別子は、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、および第１の機関の秘密鍵による署名から構成され、

個人識別子は、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、

発信者と着信者の１対１対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項２５】　個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

個別化アクセスチケットは、発信者Index 、所有者Index 、移転制御情報、発信者役割識別子、１個以上の着信者役割識別子、および有効期限情報から構成され、

役割識別子は、個人識別子、暗号化された位置情報、第４の機関のホスト個人

情報、および第１の機関の秘密鍵による署名から構成され、

個人識別子は、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、

発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項２６】　個別化アクセスチケット変更権(Enabler）を記録したコンピュータで読み取り可能な記録媒体であって、

個別化アクセスチケット変更権(Enabler）は、個別化アクセスチケット変更権(Enabler）であることを一意に表す文字列、役割識別子、および第１の機関の秘密鍵による署名から構成され、

役割識別子は、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、および第１の機関の秘密鍵による署名から構成され、

個人識別子は、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、

発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項２７】　個別化アクセスチケット（ＰＡＴ）の新規生成および既存の個別化アクセスチケット（ＰＡＴ）の内容変更を行うために、Ｎｕｌｌ－ＡＩＤ（AID_{Null}）および該Ｎｕｌｌ－ＡＩＤの Enabler(Enabler of Ｎｕｌｌ－ＡＩＤまたは Enabler of AID_{Null}）を使用し、該Ｎｕｌｌ－ＡＩＤを含む演算は、

(a) 個別化アクセスチケット（ＰＡＴ）に対する新規生成（MakeＰＡＴ）、マージ（Merge ＰＡＴ）、分割（Split ＰＡＴ）、変更（Trans ＰＡＴ）からなる演算規則に従い、

(b) Ｎｕｌｌ－ＡＩＤにのみ適用可能な規則として、

ｉ．Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知であり、

ii. Enabler of Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知である

ことを特徴とする接続制御方法。

【請求項２８】　前記Ｎｕｌｌ－ＡＩＤは、個別化アクセスチケット（ＰＡＴ）の所有者ＡＩＤとしてのみ使用可能であり、

【数１】

$$PAT<AID_{Null} \mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$$

は許可することを特徴とする請求項２７記載の接続制御方法。

【請求項２９】　Ｇｏｄ－ＡＩＤ（AID_{God}）を用いて、個別化アクセスチケット（ＰＡＴ）に読取専用属性を設定し、該Ｇｏｄ－ＡＩＤに関する演算は、

(a) Ｇｏｄ－ＡＩＤは、すべてのユーザに既知であり、

(b) Ｇｏｄ－ＡＩＤに関する演算は、

【数２】

i. $AID_{所有者}$がAID_{Null}でもAID_{God}でもない場合：

$$PAT<AID_{所有者} \mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}> + \text{Enabler of } AID_{所有者}$$

$$\rightarrow PAT<AID_{God} \mid AID_{所有者}, AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$$

ii. $AID_{所有者}$がAID_{Null}の場合：

$$PAT<AID_{Null} \mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}> + \text{Enabler of } AID_{Null}$$

$$\rightarrow PAT<AID_{God} \mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$$

である場合のいずれかのみ許可されることを特徴とする接続制御方法。

【請求項３０】　個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Ｎｕｌｌ－ＡＩＤは、Ｎｕｌｌ－ＡＩＤであることを表す文字列および該文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項３１】　個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Enabler of Ｎｕｌｌ－ＡＩＤは、Enabler であることを表す文字列、Ｎｕｌｌ－ＡＩＤの実体、および前記Enabler であることを表す文字列と前記Ｎｕｌｌ－ＡＩＤの実体を連結した文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項３２】　個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Ｇｏｄ－ＡＩＤは、Ｇｏｄ－ＡＩＤであることを表す文字列および前記Ｇｏｄ－ＡＩＤであることを表す文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項３３】　通信網におけるユーザ個人を隠蔽した通信の接続制御方法であって、

第１の機関がユーザの特性を識別する第１の機関の付与情報をユーザに付与し、

第２の機関が前記第１の機関の付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定し、

第３の機関がアクセス権を示すリンク指定型個別化アクセスチケットを発行し、

第４の機関が発信者からの発信要求に対して前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うこと

を特徴とする接続制御方法。

【請求項３４】　前記第１の機関の付与情報がリンク情報付き役割識別子であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが発信者役割識別子のリンク情報、着信者役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型１対１個別化アクセスチケット

であり、

第４の機関は発信者からの接続要求を、前記リンク情報付き役割識別子、前記リンク指定型１対１個別化アクセスチケット、および前記リンク指定型１対１個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子のリンク情報がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを特徴とする請求項３３記載の接続制御方法。

【請求項３５】　前記第１の機関の付与情報が発信者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler）であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と１個以上の着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが所有者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ個別化アクセスチケットであり、

第４の機関は発信者からの接続要求を、前記発信者リンク情報付き役割識別子、前記リンク指定型１対Ｎ個別化アクセスチケット、および前記リンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを特徴とする請求項３３記載の接続制御方法。

【請求項３６】　前記リンク指定型個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストにそのチケットを登録している場合は、第４の機関は当該接続要求を拒否することを特徴と

する請求項３３または３４または３５記載の接続制御方法。

【請求項３７】　アクセス権を示す情報であるリンク指定型個別化アクセスチケットを用いて、ユーザ間の通信を制御する接続制御方法であって、

前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを特徴とする接続制御方法。

【請求項３８】　前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型１対１個別化アクセスチケットであり、

前記リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項３７記載の接続制御方法。

【請求項３９】　前記個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ個別化アクセスチケットであり、

第４の機関が発信者からの接続要求に対して、発信者リンク情報付き役割識別子、１個以上の着信者リンク情報付き役割識別子、リンク指定型１対Ｎ個別化アクセスチケット、およびリンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項３７記載の接続制御方法。

【請求項４０】　前記検証結果が正しくても、リンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを特

徴とする請求項３７記載の接続制御方法。

【請求項４１】　個別化アクセスチケット変更権(Enabler) により第３の機関において所有者を変更する方法であって、

第１のリンク指定型個別化アクセスチケットのリンク情報で特定される所有者リンク情報付き役割識別子を第１の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler) および第１のリンク情報付き役割識別子により新たな所有者リンク情報付き役割識別子を変更し、第３のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御方法。

【請求項４２】　個別化アクセスチケット変更権(Enabler) により第３の機関において会員を追加する方法であって、

所有者が同一である複数の第４のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子をそれぞれ第３の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、前記第３の個別化アクセスチケット変更権を用いて、前記所有者リンク情報付き役割識別子と前記すべての第４のリンク指定型個別化アクセスチケットのすべての会員リンク情報付き役割識別子から構成される第５のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御方法。

【請求項４３】　個別化アクセスチケット変更権(Enabler) により第３の機関において会員を分割するときの接続制御方法であって、

第６のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第４の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、第４の個別化アクセスチケット変更権を用いて、前記所有者リンク情報付き役割識別子と前記第６のリンク指定型個別化アクセスチケットの一部の会員リンク情報付き役割識別子から構成される第７のリンク指定型個別化アクセスチケットを複数作成することを特徴とする接続制御方法。

【請求項４４】　個別化アクセスチケット変更権(Enabler) により第３の機関においてリンク指定型個別化アクセスチケットを新規生成するときの接続制御方法であって、

新規生成するリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子とするリンク情報付き役割識別子と、会員リンク情報付き役割識別子とするすべての第５のリンク情報付き役割識別子について、それぞれのリンク情報付き役割識別子の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第４のリンク情報付き役割識別子を所有者リンク情報付き役割識別子とするリンク指定型個別化アクセスチケットを新規生成することを特徴とする接続制御方法。

【請求項４５】　通信網においてユーザ個人を隠蔽した通信を制御可能とする通信網であって、

ユーザの特性を識別する付与情報をユーザに付与する第１の機関と、

前記付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定する第２の機関と、

アクセス権を示すリンク指定型個別化アクセスチケットを発行する第３の機関と、

発信者からの発信要求に対して前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う第４の機関と

を有することを特徴とする通信網。

【請求項４６】　前記第１の機関の付与情報がリンク情報付き役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型１対１個別化アクセスチケットであり、

前記第４の機関は発信者からの接続要求を、前記リンク情報付き役割識別子、前記リンク指定型１対１個別化アクセスチケット、および前記リンク指定型１対１個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対１個別化アクセスチケットが改竄されていないことを、発信者リンク情報付

き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを特徴とする請求項４５記載の通信網。

【請求項４７】　前記第１の機関の付与情報が発信者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler) であり、前記発信者の指定情報が所有者リンク情報付き役割識別子と１個以上の着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが所有者リンク情報付き役割識別子のリンク情報、１個以上の会員リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク１対Ｎ個別化アクセスチケットであり、

第４の機関は発信者からの接続要求を、前記発信者リンク情報付き役割識別子、前記リンク指定型１対Ｎ個別化アクセスチケット、および前記リンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを特徴とする請求項４５記載の通信網。

【請求項４８】　前記第４の機関は、前記リンク指定型個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストに該リンク指定型個別化アクセスチケットを登録している場合は、第４の機関は当該接続要求を拒否する拒否手段を有することを特徴とする請求項４５または４６または４７記載の通信網。

【請求項４９】　アクセス権を示す情報であるリンク指定型個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法を実施するプログラムを記録した記録媒体であって、

前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項５０】　前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型１対１個別化アクセスチケットであり、

リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク情報付き１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項４９記載の接続制御プログラムを記録した記録媒体。

【請求項５１】　前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ個別化アクセスチケットであり、

第４の機関が発信者からの接続要求を、発信者リンク情報付き役割識別子、１個以上の着信者リンク情報付き役割識別子、リンク指定型１対Ｎ個別化アクセスチケット、およびリンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子が個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項４９記載の接続制御プログラムを記録した記録媒体。

【請求項５２】　前記検証結果が正しくても、リンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを特徴とする請求項４９記載の接続制御プログラムを記録した記録媒体。

【請求項５３】　個別化アクセスチケット変更権(Enabler) により第３の機関において所有者を変更する方法を実施するプログラムを記録した記録媒体であって、

第１のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第１の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler) および第１のリンク情報付き役割識別子により新たに発信者リンク情報付き役割識別子を変更し、第３のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項５４】　個別化アクセスチケット変更権(Enabler) により第３の期間において会員を追加する方法を実施するプログラムを記録した記録媒体であって、

第４のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第３の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、１個以上の第４の個別化アクセスチケット変更権(Enabler) 、１個以上の第２のリンク情報付き役割識別子により１個以上の新たな着信者リンク情報付き役割識別子に追加し、第５のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項５５】　個別化アクセスチケット変更権(Enabler) により第３の機関において会員を削除する方法を実施するプログラムを記録した記録媒体であって、

第６のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第４の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、１個以上の第５の個別化アクセスチケット変更権(Enabler) 、１個以上の第３のリンク情報付き役割識別子により１個以上の着信者リンク情報付き役割識別子を削除し、第７のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項５６】　リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

リンク指定型個別化アクセスチケットは、発信者フラグ、移転制御フラグ、発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、有効期限、および第３の機関の秘密鍵による署名から構成されるリンク指定型１対１個別化アクセスチケットであり、

リンク情報付き役割識別子は、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、リンク情報および第１の機関の秘密鍵による署名から構成され、

個人識別子は、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、

発信者と着信者の１対１対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項５７】　リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

リンク指定型個別化アクセスチケットは、発信者Index 、所有者Index 、移転制御情報、発信者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、および有効期限情報から構成されるリンク指定型１対Ｎ個別化アクセスチケットであり、

リンク情報付き役割識別子は、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、リンク情報、および第１の機関の秘密鍵による署名から構成され、

個人識別子は、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、

発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項５８】　個別化アクセスチケット変更権(Enabler) を記録したコンピュータで読み取り可能な記録媒体であって、

個別化アクセスチケット変更権(Enabler) は、個別化アクセスチケット変更権(Enabler) であることを一意に表す文字列、役割識別子、および第１の機関の秘密鍵による署名から構成され、

リンク情報付き役割識別子は、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、リンク情報、および第１の機関の秘密鍵による署名から構成され、

個人識別子は、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、

発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項５９】　リンク指定型個別化アクセスチケット（ＰＡＴ）の新規生成および既存のリンク指定型個別化アクセスチケット（ＰＡＴ）の内容変更を行うため、Ｎｕｌｌ－ＡＩＤ（AID_{Null}）および該Ｎｕｌｌ－ＡＩＤの Enabler (Enabler of Ｎｕｌｌ－ＡＩＤまたは Enabler of AID_{Null}）を使用し、該Ｎｕｌｌ－ＡＩＤを含む演算は、

(a) リンク指定型個別化アクセスチケット（ＰＡＴ）に対する新規生成（Make ＰＡＴ）、マージ（Merge ＰＡＴ）、分割（Split ＰＡＴ）、変更（Trans ＰＡＴ）からなる演算規則に従い、

(b) Ｎｕｌｌ－ＡＩＤにのみ適用可能な規則として、

ｉ．Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知であり、

ii. Enabler of Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知である

ことを特徴とする接続制御方法。

【請求項６０】　前記Ｎｕｌｌ－ＡＩＤは、リンク指定型個別化アクセスチケット（ＰＡＴ）の所有者ＡＩＤとしてのみ使用可能であり、

【数３】

$PAT<AID_{Null} \mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

は許可することを特徴とする請求項５９記載の接続制御方法。

【請求項６１】　Ｇｏｄ－ＡＩＤ（AID_{God}）を用いて、リンク指定型個別化アクセスチケット（ＰＡＴ）に読取専用属性を設定し、該Ｇｏｄ－ＡＩＤに関する演算は、

(a) Ｇｏｄ－ＡＩＤは、すべてのユーザに既知であり、

(b) Ｇｏｄ－ＡＩＤに関する演算は、

【数４】

ｉ．$AID_{所有者}$がAID_{Null}でもAID_{God}でもない場合：

$PAT<AID_{所有者}|AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

$+$ Enabler of $AID_{所有者}$

$\rightarrow PAT<AID_{God}|AID_{所有者}, AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

ii．$AID_{所有者}$がAID_{Null}の場合：

$PAT<AID_{Null}|AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

$+$ Enabler of AID_{Null}

$\rightarrow PAT<AID_{God}|AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

である場合のいずれかのみ許可されることを特徴とする接続制御方法。

【請求項６２】　リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Ｎｕｌｌ－ＡＩＤは、Ｎｕｌｌ－ＡＩＤであることを表す文字列および該文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項６３】　リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Enabler of Ｎｕｌｌ－ＡＩＤは、Enabler であることを表す文字列、Ｎｕｌｌ－ＡＩＤの実体、および前記Enabler であることを表す文字列と前記Ｎｕｌｌ－ＡＩＤの実体を連結した文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項６４】　リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Ｇｏｄ－ＡＩＤは、Ｇｏｄ－ＡＩＤであることを表す文字列および前記Ｇｏｄ－ＡＩＤであることを表す文字列に対して認証局の署名を施したものであること

を特徴とするデータ構造を記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信網において着信者の通信網における識別子を隠蔽しつつ、通信網における識別子を隠蔽した他のユーザからの通信の接続を制御する接続制御方法および通信網と接続制御プログラムおよびデータ構造を記録した記録媒体に関する。

【０００２】

【従来の技術】

近年、電話やコンピュータネットワークを用いた個人攻撃、例えば嫌がらせ、名誉毀損等が深刻な社会問題になっている。このような個人攻撃は通信網を介して氏名、性別、年齢、電話番号、電子メールアドレスといったプライバシー情報が第三者に漏洩するために発生するものである。具体的には、第三者による盗聴、偽装等の盗難、第三者による意図的な収集（アンケート）、発信者の間違い電話等の端末操作ミス、発信者によるやむを得ない公開（情報誌、電子掲示板、ホームページ等）がある。

【０００３】

現在、盗難対策には認証、暗号化があり、間違い電話対策には端末の電話帳機能がある。また、第三者によるアンケート等の意図的な収集および発信者によるやむを得ない公開に対しては、いくつかの対策が実施されているが、いずれも漏洩を完全に防止することはできない。

【０００４】

求人（仲間募集）や売買のように他のユーザと個人的に連絡を取る必要があるユーザは、最低限、氏名と連絡先を情報誌、電子掲示板、またはホームページに掲載しなければならない。また、性別、年齢といったプライバシー情報を公開しなければならない場合もある。ところが、これらのメディアを閲覧するのは善意のユーザだけではない。個人攻撃を仕掛けようと企むユーザも閲覧する可能性は決して小さくない。そこで、情報を公開したユーザを何らかの手段で個人攻撃か

ら保護することが必要になる。

【０００５】

このとき、そのユーザの取り得る戦略は２種類ある。ひとつは情報を限定公開する戦略で、具体的にはニックネームがある。もうひとつは接続相手を着信側で限定する戦略で、具体的には二重番号登録、発信者番号通知、着信拒否、匿名電子メール(Anonymous Mails) がある。

【０００６】

インターネットやパソコン通信の電子掲示板システムではニックネーム（ハンドルネーム）による発信が可能なため、実名を隠蔽することができる。しかしながら、善意のユーザにはすべてのプライバシー情報を公開するけれども、悪意のユーザには公開しないといったような制御はできないし、発信者の電子メールアドレスも隠蔽できない。このため、第三者から攻撃される恐れがある。

【０００７】

二重番号では、図２７に示すように、回線に複数の電話番号を割り当て、そのうちの一部の番号への呼をすべて自動的に切断するため、個人攻撃を被る恐れはない。その代わり、着呼可能な番号を知る者には厳重に守秘義務が課される。

【０００８】

また、発信者番号通知は、図２８に示すように、発信者電話番号を着信側端末に通知するものであり、アナログ公衆網、ＩＳＤＮ、デジタル携帯網で提供されているが、番号非通知の場合には、着信端末にも何も表示されない。

【０００９】

一方、着信拒否は、図２９に示すように、呼を自動的に切断する機能であり、アナログ公衆網、ＩＳＤＮ、デジタル携帯網で提供されている。仕様は網によって異なる。アナログ公衆網とＩＳＤＮでは、着信側回線あるいは端末で指定した発信者番号の呼以外は接続しない。逆に、デジタル携帯網では、着信側端末で設定した発信者番号の呼を切断する。

【００１０】

一般に、発信者番号通知と着信拒否は組み合わせて利用される。ところが、両者を組み合わせると、発信者と着信者のいずれか一方しか保護できなくなる。ア

ナログ公衆網やＩＳＤＮでは番号非通知の呼を切断するため、番号漏洩を防止できなくなる。仕様を逆手にとると、個人情報の収集手段として利用できるからである。一方、デジタル携帯網では番号非通知の呼を切断しないため、着信者を個人攻撃から保護できなくなる。

【００１１】

匿名電子メールでは、図３０に示すように、発信者メールアドレスをリメーラ（remailer）機能を持つメールサーバのメールアドレスに書き換えて送信先に転送する。このように、発信者メールアドレスを隠蔽するため、発信者メールアドレスの漏洩を防ぐことができる。その一方で、匿名による攻撃が可能になるため、着信者が第三者から攻撃される危険性はより高くなる。

【００１２】

これを防ぐために、着信者から要求があった場合には、リメーラはその着信者宛の匿名メールの配信を中止する。ところが、この機能を用いると番号漏洩を防ぐことはできなくなる。着信拒否同様、個人情報の収集手段として利用できるからである。

【００１３】

【発明が解決しようとする課題】

上述したように、従来のニックネーム、二重番号登録、発信者番号通知、着信拒否、匿名電子メール等の方法では、それぞれ発信者の電子メールアドレスを隠蔽できず、第三者から攻撃されたり、着呼可能番号を知る者に厳重な守秘義務が課せられたり、番号非通知の呼を切断しない場合もあり、着信者を個人攻撃から保護できなかったり、匿名による攻撃が可能となり、着信者が第三者から攻撃される危険性が高くなるというような種々の問題がある。

【００１４】

本発明は、上記に鑑みてなされたもので、その目的とするところは、第三者による意図的な収集およびユーザによるやむを得ない公開に対して匿名性とセキュリティを確保すべく発信者および着信者の匿名性を保持しつつ発信者からの通信の接続を可能とし、着信者が匿名性を悪用した発信者による攻撃にさらされた場合には、その攻撃による着信者への被害を食い止めることを可能とする接続制御

方法および通信網と接続制御プログラムおよびデータ構造を記録した記録媒体を提供することにある。

【００１５】

【課題を解決するための手段】

上記目的を達成するため、請求項１記載の本発明は、通信網におけるユーザ個人を隠蔽した通信の接続制御方法であって、第１の機関がユーザの特性を識別する第１の機関の付与情報をユーザに付与し、第２の機関が前記第１の機関の付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定し、第３の機関がアクセス権を示す個別化アクセスチケットを発行し、第４の機関が発信者からの発信要求に対して前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うことを要旨とする。

【００１６】

請求項１記載の本発明にあっては、第１の機関の付与情報をユーザに付与し、第１の機関の付与情報とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示す個別化アクセスチケットを発行し、発信者からの発信要求に対して個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う。

【００１７】

また、請求項２記載の本発明は、請求項１記載の発明において、前記第１の機関の付与情報が役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含む１対１個別化アクセスチケットであり、第４の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検

証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【００１８】

請求項２記載の本発明にあっては、第１の機関の付与情報は役割識別子であり、発信者の指定情報は発信者役割識別子と着信者役割識別子であり、個別化アクセスチケットは発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、有効期限を含む１対１個別化アクセスチケットであり、役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【００１９】

更に、請求項３記載の本発明は、請求項１記載の発明において、前記第１の機関の付与情報が発信者役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が発信者役割識別子と１個以上の着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含む１対Ｎ個別化アクセスチケットであり、第４の機関は発信者からの接続要求を、前記発信者役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【００２０】

請求項３記載の本発明にあっては、第１の機関の付与情報は発信者役割識別子

と個別化アクセスチケット変更権(Enabler) であり、発信者の指定情報は発信者役割識別子と１個以上の着信者役割識別子であり、個別化アクセスチケットは発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含む１対Ｎ個別化アクセスチケットであり、発信者役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【００２１】

請求項４記載の本発明は、請求項１または２または３記載の発明において、前記個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストにそのチケットを登録している場合は、第４の機関は当該接続要求を拒否することを要旨とする。

【００２２】

請求項４記載の本発明にあっては、個別化アクセスチケットに関する認証結果が正しくても、着信者の個別化アクセスチケットが着信拒否リストに登録している場合は、接続要求を拒否する。

【００２３】

また、請求項５記載の本発明は、アクセス権を示す情報である個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法において、前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを要旨とする。

【００２４】

請求項５記載の本発明にあっては、個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する。

【００２５】

更に、請求項６記載の本発明は、請求項５記載の発明において、前記個別化ア

クセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを要旨とする。

【００２６】

請求項６記載の本発明にあっては、個別化アクセスチケットは発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、有効期限を含み、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う。

【００２７】

請求項７記載の本発明は、請求項５記載の発明において、前記個別化アクセスチケットが発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含み、第４の機関が発信者からの接続要求に対して、発信者役割識別子、１個以上の着信者役割識別子、個別化アクセスチケット、および個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを要旨とする。

【００２８】

請求項７記載の本発明にあっては、個別化アクセスチケットが発信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含み、発信者役割識別子、１個以上の着信者役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３

要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求に対してユーザ間の接続を行う。

【００２９】

また、請求項８記載の本発明は、請求項５記載の発明において、前記検証結果が正しくても、個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを要旨とする。

【００３０】

請求項８記載の本発明にあっては、検証結果が正しくても個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する。

【００３１】

更に、請求項９記載の本発明は、個別化アクセスチケット変更権(Enabler）により第３の機関において所有者を変更するときの接続制御方法であって、第１の個別化アクセスチケットの所有者役割識別子を第１の個別化アクセスチケット変更権(Enabler）で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler）および第１の役割識別子により新たな所有者役割識別子を変更し、第３の個別化アクセスチケットを作成することを要旨とする。

【００３２】

請求項９記載の本発明にあっては、第１の個別化アクセスチケットの所有者役割識別子を第１の個別化アクセスチケット変更権(Enabler）で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler）および第１の役割識別子により新たな所有者役割識別子を変更し、第３の個別化アクセスチケットを作成する。

【００３３】

請求項１０記載の本発明は、個別化アクセスチケット変更権(Enabler）により第３の機関において会員を追加するときの接続制御方法であって、所有者が同一である複数の第４の個別化アクセスチケットの所有者役割識別子をそれぞれ第３の個別化アクセスチケット変更権(Enabler）と照合し、正しい場合に、前記第３の個別化アクセスチケット変更権を用いて、前記所有者役割識別子と前記すべての第４の個別化アクセスチケットのすべての会員役割識別子から構成される第５

の個別化アクセスチケットを作成することを要旨とする。

【００３４】

請求項１０記載の本発明にあっては、第４の個別化アクセスチケットの所有者役割識別子を第３の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、１個以上の第４の個別化アクセスチケット変更権(Enabler) 、１個以上の第２の役割識別子により１個以上の新たな会員役割識別子に追加すなわち連結し、第５の個別化アクセスチケットを作成する。

【００３５】

尚、同一所有者役割識別子の複数個別化アクセスチケットをマージする演算は

【数５】

$$PAT<AID_{所有者} \mid AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}>$$

$$+PAT<AID_{所有者} \mid AID_{会員b1}, AID_{会員b2}, \cdots, AID_{会員bN}>$$

$$+ \text{Enabler of } AID_{所有者}$$

$$\longrightarrow$$

$$PAT<AID_{所有者} \mid AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}$$

$$AID_{会員b1}, AID_{会員b2}, \cdots, AID_{会員bN}>$$

である。

【００３６】

また、請求項１１記載の本発明は、個別化アクセスチケット変更権(Enabler) により第３の機関において会員を分割するときの接続制御方法であって、第６の個別化アクセスチケットの所有者役割識別子を第４の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、前記第４の個別化アクセスチケット変更権を用いて、前記所有者役割識別子と前記第６の個別化アクセスチケットの一部の会員役割識別子から構成される第７の個別化アクセスチケットを複数作成することを要旨とする。

【００３７】

請求項１１記載の本発明にあっては、第６の個別化アクセスチケットの所有者

役割識別子を第４の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、１個以上の第５の個別化アクセスチケット変更権(Enabler) 、１個以上の第３の役割識別子により１個以上の会員役割識別子を分割、具体的には例えば削除し、第７の個別化アクセスチケットを作成する。

【００３８】

尚、個別化アクセスチケットを同一所有者役割識別子の複数個別化アクセスチケットに分割する演算は、

【数６】

$$PAT<AID_{所有者} \mid AID_{会員a1'}, AID_{会員a2'}, \cdots, AID_{会員aN'}$$
$$AID_{会員b1'}, AID_{会員b2'}, \cdots, AID_{会員bN'}>$$
$$+ \text{Enabler of } AID_{所有者}$$
$$\longrightarrow$$
$$PAT<AID_{所有者} \mid AID_{会員a1'}, AID_{会員a2'}, \cdots, AID_{会員aN'}>$$
$$+PAT<AID_{所有者} \mid AID_{会員b1'}, AID_{会員b2'}, \cdots, AID_{会員bN'}>$$

である。

【００３９】

また、請求項１２記載の本発明は、個別化アクセスチケット変更権(Enabler) により第３の機関において個別化アクセスチケットを新規生成するときの接続制御方法であって、新規生成する個別化アクセスチケットの所有者役割識別子とする役割識別子と、会員役割識別子とするすべての第５の役割識別子について、それぞれの役割識別子の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第４の役割識別子を所有者役割識別子とする個別化アクセスチケットを新規生成することを要旨とする。

【００４０】

請求項１２記載の本発明にあっては、これから新規生成する個別化アクセスチケットの第５の所有者役割識別子とする第４の役割識別子と、会員役割識別子とするすべての第５の役割識別子について、それぞれの役割識別子の個別化アクセ

スチケット変更権(Enabler) で照合し、照合結果が、正しい場合に、第４の役割識別子を所有者役割識別子とする個別化アクセスチケットを新規生成する。

【００４１】

更に、請求項１３記載の本発明は、通信網においてユーザ個人を隠蔽した通信を制御可能とする通信網であって、ユーザの特性を識別する付与情報をユーザに付与する第１の機関と、前記付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定する第２の機関と、アクセス権を示す個別化アクセスチケットを発行する第３の機関と、発信者からの発信要求に対して前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う第４の機関とを有することを要旨とする。

【００４２】

請求項１３記載の本発明にあっては、付与情報をユーザに付与し、付与情報とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示す個別化アクセスチケットを発行し、発信者からの発信要求に対して個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う。

【００４３】

請求項１４記載の本発明は、請求項１３記載の発明において、前記第１の機関の付与情報が役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、前記第４の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを要旨とする。

【００４４】

請求項１４記載の本発明にあっては、第１の機関の付与情報は役割識別子であり、発信者の指定情報は発信者役割識別子と着信者役割識別子であり、個別化アクセスチケットは発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、有効期限を含み、役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【００４５】

また、請求項１５記載の本発明は、請求項１３記載の発明において、前記第１の機関の付与情報が発信者役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が発信者役割識別子と１個以上の着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含み、第４の機関は発信者からの接続要求を、前記発信者役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを要旨とする。

【００４６】

請求項１５記載の本発明にあっては、第１の機関の付与情報は発信者役割識別子と個別化アクセスチケット変更権(Enabler)であり、発信者の指定情報は発信者役割識別子と１個以上の着信者役割識別子であり、個別化アクセスチケットは発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含み、発信者役割識別子、個別化アクセ

スチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【００４７】

更に、請求項１６記載の本発明は、請求項１３または１４または１５記載の発明において、前記第４の機関が、前記個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストに該個別化アクセスチケットを登録している場合は、第４の機関は当該接続要求を拒否する拒否手段を有することを要旨とする。

【００４８】

請求項１６記載の本発明にあっては、個別化アクセスチケットに関する認証結果が正しくても、着信者が着信拒否リストに該個別化アクセスチケットを登録している場合は、当該接続要求を拒否する。

【００４９】

請求項１７記載の本発明は、アクセス権を示す情報である個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法を実施するプログラムを記録した記録媒体であって、前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する接続制御プログラムを記録媒体に記録することを要旨とする。

【００５０】

請求項１７記載の本発明にあっては、個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【００５１】

また、請求項１８記載の本発明は、請求項１７記載の発明において、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移

転制御フラグ、および有効期限を含み、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録することを要旨とする。

【００５２】

請求項１８記載の本発明にあっては、個別化アクセスチケットは発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、有効期限を含み、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【００５３】

更に、請求項１９記載の本発明は、請求項１７記載の発明において、前記個別化アクセスチケットが発信者役割識別子、１個以上の着信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含み、第４の機関が発信者からの接続要求を、発信者役割識別子、１個以上の着信者役割識別子、個別化アクセスチケット、および個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録することを要旨とする。

【００５４】

請求項１９記載の本発明にあっては、個別化アクセスチケットが発信者役割識別子、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含み、発信者役割識別子、１個以上の着信者役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセス

チケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求に対してユーザ間の接続を行う接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【００５５】

請求項２０記載の本発明は、請求項１７記載の発明において、前記検証結果が正しくても、個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する接続制御プログラムを記録媒体に記録することを要旨とする。

【００５６】

請求項２０記載の本発明にあっては、検証結果が正しくても個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【００５７】

また、請求項２１記載の本発明は、個別化アクセスチケット変更権(Enabler)により第３の機関において所有者を変更する方法を実施するプログラムを記録した記録媒体であって、第１の個別化アクセスチケットの発信者役割識別子を第１の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler)および第１の役割識別子により新たに発信者役割識別子を変更し、第３の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【００５８】

請求項２１記載の本発明にあっては、第１の個別化アクセスチケットの発信者役割識別子を第１の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler)および第１の役割識別子により新たな発信者役割識別子を変更し、第３の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、そ

の流通性を高めることができる。

【００５９】

更に、請求項２２記載の本発明は、個別化アクセスチケット変更権(Enabler)により第３の機関において会員を追加する方法を実施するプログラムを記録した記録媒体であって、第４の個別化アクセスチケットの発信者役割識別子を第３の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、１個以上の第４の個別化アクセスチケット変更権(Enabler)、１個以上の第２の役割識別子により１個以上の新たな着信者役割識別子に追加し、第５の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【００６０】

請求項２２記載の本発明にあっては、第４の個別化アクセスチケットの発信者役割識別子を第３の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、１個以上の第４の個別化アクセスチケット変更権(Enabler)、１個以上の第２の役割識別子により１個以上の新たな着信者役割識別子に追加し、第５の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【００６１】

請求項２３記載の本発明は、個別化アクセスチケット変更権(Enabler)により第３の機関において会員を削除する方法を実施するプログラムを記録した記録媒体であって、第６の個別化アクセスチケットの発信者役割識別子を第４の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、１個以上の第５の個別化アクセスチケット変更権(Enabler)、１個以上の第３の役割識別子により１個以上の着信者役割識別子を削除し、第７の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【００６２】

請求項２３記載の本発明にあっては、第６の個別化アクセスチケットの発信者役割識別子を第４の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、１個以上の第５の個別化アクセスチケット変更権(Enabler)、１個以上の第３の役割識別子により１個以上の着信者役割識別子を削除し、第７の個別化

アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【００６３】

また、請求項２４記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、個別化アクセスチケットが、発信者フラグ、移転制御フラグ、発信者役割識別子、着信者役割識別子、有効期限、および第３の機関の秘密鍵による署名から構成され、役割識別子が、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、および第１の機関の秘密鍵による署名から構成され、個人識別子が、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、発信者と着信者の１対１対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【００６４】

請求項２４記載の本発明にあっては、発信者フラグ、移転制御フラグ、発信者役割識別子、着信者役割識別子、有効期限、および第３の機関の秘密鍵による署名から構成される個別化アクセスチケットを発信者と着信者の１対１対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００６５】

更に、請求項２５記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、個別化アクセスチケットが、発信者Index 、所有者Index 、移転制御情報、発信者役割識別子、１個以上の着信者役割識別子、および有効期限情報から構成され、役割識別子が、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、および第１の機関の秘密鍵による署名から構成され、個人識別子が、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、発信者と着信者の１対N対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【００６６】

請求項２５記載の本発明にあっては、発信者Index 、所有者Index 、移転制御情報、発信者役割識別子、１個以上の着信者役割識別子、および有効期限情報から構成される個別化アクセスチケットを発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００６７】

請求項２６記載の本発明は、個別化アクセスチケット変更権(Enabler) を記録したコンピュータで読み取り可能な記録媒体であって、個別化アクセスチケット変更権(Enabler) が、個別化アクセスチケット変更権(Enabler) であることを一意に表す文字列、役割識別子、および第１の機関の秘密鍵による署名から構成され、役割識別子が、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、および第１の機関の秘密鍵による署名から構成され、個人識別子が、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【００６８】

請求項２６記載の本発明にあっては、個別化アクセスチケット変更権(Enabler) であることを一意に表す文字列、役割識別子、および第１の機関の秘密鍵による署名から構成される個別化アクセスチケット変更権(Enabler) を発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００６９】

請求項２７記載の本発明は、個別化アクセスチケット（ＰＡＴ）の新規生成および既存の個別化アクセスチケット（ＰＡＴ）の内容変更を行うために、Ｎｕｌｌ－ＡＩＤ（AID_{Null}）および該Ｎｕｌｌ－ＡＩＤの Enabler(Enabler of Ｎｕｌｌ－ＡＩＤまたは Enabler of AID_{Null}）を使用し、該Ｎｕｌｌ－ＡＩＤを含む演算が、

(a) 個別化アクセスチケット（ＰＡＴ）に対する新規生成（MakeＰＡＴ）、マージ（Merge ＰＡＴ）、分割（Split ＰＡＴ）、変更（Trans ＰＡＴ）からなる演算規則に従い、

(b) Ｎｕｌｌ－ＡＩＤにのみ適用可能な規則として、

ｉ．Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知であり、

ii. Enabler of Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知であることを要旨とする。

【００７０】

請求項２７記載の本発明にあっては、個別化アクセスチケット（ＰＡＴ）の新規生成および既存の個別化アクセスチケット（ＰＡＴ）の内容変更を行うために、Ｎｕｌｌ－ＡＩＤ（$ＡＩＤ_{Null}$）および該Ｎｕｌｌ－ＡＩＤの Enabler(Enabler of Ｎｕｌｌ－ＡＩＤまたは Enabler of $ＡＩＤ_{Null}$）を使用するため、会員ＡＩＤおよび Enabler of 会員ＡＩＤを所有者ＡＩＤに渡さなくても新規生成（MakeＰＡＴ）およびマージ（Merge ＰＡＴ）を行うことができる。

【００７１】

また、請求項２８記載の本発明は、請求項２７記載の発明において、前記Ｎｕｌｌ－ＡＩＤが、個別化アクセスチケット（ＰＡＴ）の所有者ＡＩＤとしてのみ使用可能であり、

【数７】

$$ＰＡＴ<ＡＩＤ_{Null}|ＡＩＤ_{会員1}，ＡＩＤ_{会員2}，…，ＡＩＤ_{会員N}>$$

は許可することを要旨とする。

【００７２】

請求項２８記載の本発明にあっては、Ｎｕｌｌ－ＡＩＤは個別化アクセスチケット（ＰＡＴ）の所有者ＡＩＤとしてのみ使用可能であり、

【数８】

$$ＰＡＴ<ＡＩＤ_{Null}|ＡＩＤ_{会員1}，ＡＩＤ_{会員2}，…，ＡＩＤ_{会員N}>$$

は許可するため、$ＰＡＴ<ＡＩＤ_{所有者}|ＡＩＤ_{会員}>$の所有者が$ＡＩＤ_{会員}$の Enabler を知らない場合には、このＰＡＴから$ＰＡＴ<ＡＩＤ_{Null}|ＡＩＤ_{会員}>$を作成することはできない。

【００７３】

更に、請求項２９記載の本発明は、Ｇｏｄ－ＡＩＤ（$ＡＩＤ_{God}$）を用いて、個別化アクセスチケット（ＰＡＴ）に読取専用属性を設定し、該Ｇｏｄ－ＡＩＤに関する演算が、

(a) Ｇｏｄ－ＡＩＤは、すべてのユーザに既知であり、

(b) Ｇｏｄ－ＡＩＤに関する演算が、

【数９】

ｉ．$ＡＩＤ_{所有者}$が$ＡＩＤ_{Null}$でも$ＡＩＤ_{God}$でもない場合：

$ＰＡＴ＜ＡＩＤ_{所有者} | ＡＩＤ_{会員1}, ＡＩＤ_{会員2}, \cdots, ＡＩＤ_{会員N}＞$

＋ Enabler of $ＡＩＤ_{所有者}$

$\rightarrow ＰＡＴ＜ＡＩＤ_{God} | ＡＩＤ_{所有者}, ＡＩＤ_{会員1}, ＡＩＤ_{会員2}, \cdots, ＡＩＤ_{会員N}＞$

ｉｉ．$ＡＩＤ_{所有者}$が$ＡＩＤ_{Null}$の場合：

$ＰＡＴ＜ＡＩＤ_{Null} | ＡＩＤ_{会員1}, ＡＩＤ_{会員2}, \cdots, ＡＩＤ_{会員N}＞$

＋ Enabler of $ＡＩＤ_{Null}$

$\rightarrow ＰＡＴ＜ＡＩＤ_{God} | ＡＩＤ_{会員1}, ＡＩＤ_{会員2}, \cdots, ＡＩＤ_{会員N}＞$

である場合のいずれかのみ許可されることを要旨とする。

【００７４】

請求項２９記載の本発明にあっては、Ｇｏｄ－ＡＩＤ（$ＡＩＤ_{God}$）を用いて、個別化アクセスチケット（ＰＡＴ）に読取専用属性を設定するため、グループ通信において参加者を固定することができる。

【００７５】

更に、請求項３０記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、Ｎｕｌｌ－ＡＩＤが、Ｎｕｌｌ－ＡＩＤであることを表す文字列および該文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【００７６】

請求項３０記載の本発明にあっては、Ｎｕｌｌ－ＡＩＤであることを表す文字列および該文字列に対して認証局の署名を施したものからなるデータ構造のＮｕｌｌ－ＡＩＤを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００７７】

請求項３１記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、 Enabler of Ｎｕｌｌ－ＡＩＤは、Enabler であることを表す文字列、Ｎｕｌｌ－ＡＩＤの実体、および前記Enabler であることを表す文字列と前記Ｎｕｌｌ－ＡＩＤの実体を連結した文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【００７８】

請求項３１記載の本発明にあっては、Enabler であることを表す文字列、Ｎｕｌｌ－ＡＩＤの実体、およびEnabler であることを表す文字列とＮｕｌｌ－ＡＩＤの実体を連結した文字列に対して認証局の署名を施したものからなるデータ構造の Enabler of Ｎｕｌｌ－ＡＩＤを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００７９】

また、請求項３２記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、Ｇｏｄ－ＡＩＤが、Ｇｏｄ－ＡＩＤであることを表す文字列および前記Ｇｏｄ－ＡＩＤであることを表す文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【００８０】

請求項３２記載の本発明にあっては、Ｇｏｄ－ＡＩＤであることを表す文字列およびＧｏｄ－ＡＩＤであることを表す文字列に対して認証局の署名を施したものからなるデータ構造のＧｏｄ－ＡＩＤを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００８１】

更に、請求項３３記載の本発明は、通信網におけるユーザ個人を隠蔽した通信の接続制御方法であって、第１の機関がユーザの特性を識別する第１の機関の付与情報をユーザに付与し、第２の機関が前記第１の機関の付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定し、第３の機関がアクセス権を示すリンク指定型個別化アクセスチケットを発行し、第４の機関が発信者からの発信要求に対して前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うことを要旨とする。

【００８２】

請求項３３記載の本発明にあっては、第１の機関の付与情報をユーザに付与し、第１の機関の付与情報とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示すリンク指定型個別化アクセスチケットを発行し、発信者からの発信要求に対してリンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う。

【００８３】

請求項３４記載の本発明は、請求項３３記載の発明において、前記第１の機関の付与情報がリンク情報付き役割識別子であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが発信者役割識別子のリンク情報、着信者役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型１対１個別化アクセスチケットであり、第４の機関は発信者からの接続要求を、前記リンク情報付き役割識別子、前記リンク指定型１対１個別化アクセスチケット、および前記リンク指定型１対１個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子のリンク情報がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、

検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【００８４】

請求項３４記載の本発明にあっては、第１の機関の付与情報はリンク情報付き役割識別子であり、発信者の指定情報は発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、リンク指定型個別化アクセスチケットは発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、有効期限を含むリンク指定型１対１個別化アクセスチケットであり、リンク情報付き役割識別子、リンク指定型１対１個別化アクセスチケット、リンク指定型１対１個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【００８５】

また、請求項３５記載の本発明は、請求項３３記載の発明において、前記第１の機関の付与情報が発信者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler) であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と１個以上の着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが所有者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ個別化アクセスチケットであり、第４の機関は発信者からの接続要求を、前記発信者リンク情報付き役割識別子、前記リンク指定型１対Ｎ個別化アクセスチケット、および前記リンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに

含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【００８６】

請求項３５記載の本発明にあっては、第１の機関の付与情報は所有者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler) であり、発信者の指定情報は発信者リンク情報付き役割識別子と１個以上の着信者リンク情報付き役割識別子であり、リンク指定型個別化アクセスチケットは所有者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ個別化アクセスチケットであり、発信者リンク情報付き役割識別子、リンク指定型１対Ｎ個別化アクセスチケット、リンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【００８７】

更に、請求項３６記載の本発明は、請求項３３または３４または３５記載の発明において、前記リンク指定型個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストにそのチケットを登録している場合は、第４の機関は当該接続要求を拒否することを要旨とする。

【００８８】

請求項３６記載の本発明にあっては、リンク指定型１対Ｎ個別化アクセスチケットに関する認証結果が正しくても、着信者のリンク指定型１対Ｎ個別化アクセスチケットが着信拒否リストに登録している場合は、接続要求を拒否する。

【００８９】

請求項３７記載の本発明は、アクセス権を示す情報であるリンク指定型個別化アクセスチケットを用いて、ユーザ間の通信を制御する接続制御方法であって、前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを要旨とする。

【００９０】

請求項３７記載の本発明にあっては、リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する。

【００９１】

また、請求項３８記載の本発明は、請求項３７記載の発明において、前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型１対１個別化アクセスチケットであり、前記リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを要旨とする。

【００９２】

請求項３８記載の本発明にあっては、リンク指定型個別化アクセスチケットは発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、有効期限を含むリンク指定型１対１であり、リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う。

【００９３】

更に、請求項３９記載の本発明は、請求項３７記載の発明において、前記個別

化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ個別化アクセスチケットであり、第４の機関が発信者からの接続要求に対して、発信者リンク情報付き役割識別子、１個以上の着信者リンク情報付き役割識別子、リンク指定型１対Ｎ個別化アクセスチケット、およびリンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを要旨とする。

【００９４】

請求項３９記載の本発明にあっては、リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ個別化アクセスチケットであり、所有者リンク情報付き役割識別子、１個以上の着信者リンク情報付き役割識別子、リンク指定型１対Ｎ個別化アクセスチケット、リンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求に対してユーザ間の接続を行う。

【００９５】

請求項４０記載の本発明は、請求項３７記載の発明において、前記検証結果が正しくても、リンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを要旨とする。

【００９６】

請求項４０記載の本発明にあっては、検証結果が正しくてもリンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する。

【００９７】

また、請求項４１記載の本発明は、個別化アクセスチケット変更権(Enabler)により第３の機関において所有者を変更する方法であって、第１のリンク指定型個別化アクセスチケットのリンク情報で特定される所有者リンク情報付き役割識別子を第１の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler)および第１のリンク情報付き役割識別子により新たな所有者リンク情報付き役割識別子を変更し、第３のリンク指定型個別化アクセスチケットを作成することを要旨とする。

【００９８】

請求項４１記載の本発明にあっては、第１のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第１の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler)および第１のリンク情報付き役割識別子により新たな所有者リンク情報付き役割識別子を変更し、第３のリンク指定型個別化アクセスチケットを作成する。

【００９９】

更に、請求項４２記載の本発明は、個別化アクセスチケット変更権(Enabler)により第３の機関において会員を追加する接続制御方法であって、所有者が同一である複数の第４のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子をそれぞれ第３の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、前記第３の個別化アクセスチケット変更権を用いて、前記所有者リンク情報付き役割識別子と前記すべての第４のリンク指定型個別化アクセスチケットのすべての会員リンク情報付き役割識別子から構成される第５のリンク指定型個別化アクセスチケットを作成することを要旨とする。

【０１００】

請求項４２記載の本発明にあっては、第４の個別化アクセスチケットの所有者役割識別子を第３の個別化アクセスチケット変更権(Enabler）と照合し、正しい場合に、１個以上の第４の個別化アクセスチケット変更権(Enabler）、１個以上の第２の役割識別子により１個以上の新たな会員役割識別子に追加すなわち連結し、第５の個別化アクセスチケットを作成する。

【０１０１】

なお、同一所有者役割識別子の複数個個別化アクセスチケットをマージする演算は、

【数１０】

$$PAT<AID_{所有者} \mid AID_{会員a1},\ AID_{会員a2},\ \cdots,\ AID_{会員aM}>$$

$$+PAT<AID_{所有者} \mid AID_{会員b1},\ AID_{会員b2},\ \cdots,\ AID_{会員bN}>$$

$$+\ Enabler\ of\ AID_{所有者}$$

$$\longrightarrow$$

$$PAT<AID_{所有者} \mid AID_{会員a1},\ AID_{会員a2},\ \cdots,\ AID_{会員aM},$$

$$AID_{会員b1},\ AID_{会員b2},\ \cdots,\ AID_{会員bN}>$$

である。

【０１０２】

請求項４３記載の本発明は、個別化アクセスチケット変更権(Enabler）により第３の機関において会員を分割するときの接続制御方法であって、第６のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第４の個別化アクセスチケット変更権(Enabler）と照合し、正しい場合に、第４の個別化アクセスチケット変更権を用いて、前記所有者リンク情報付き役割識別子と前記第６のリンク指定型個別化アクセスチケットの一部の会員リンク情報付き役割識別子から構成される第７のリンク指定型個別化アクセスチケットを複数作成することを要旨とする。

【０１０３】

請求項４３記載の本発明にあっては、第６のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第４の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、１個以上の第５の個別化アクセスチケット変更権(Enabler)、１個以上の第３のリンク情報付き役割識別子により１個以上の会員リンク情報付き役割識別子を分類、具体的には例えば削除し、第７のリンク指定型個別化アクセスチケットを作成する。

【０１０４】

なお、リンク指定型個別化アクセスチケットを同一所有者役割識別子の複数のリンク指定型個別化アクセスチケットに分割する演算は、

【数１１】

$$PAT<AID_{所有者} \mid AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}$$
$$AID_{会員b1}, AID_{会員b2}, \cdots, AID_{会員bN}>$$
$$+ \text{Enabler of } AID_{所有者}$$
$$\longrightarrow$$
$$PAT<AID_{所有者} \mid AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}>$$
$$+PAT<AID_{所有者} \mid AID_{会員b1}, AID_{会員b2}, \cdots, AID_{会員bN}>$$

である。

【０１０５】

また、請求項４４記載の本発明は、個別化アクセスチケット変更権(Enabler)により第３の機関においてリンク指定型個別化アクセスチケットを新規生成するときの接続制御方法であって、新規生成するリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子とするリンク情報付き役割識別子と、会員リンク情報付き役割識別子とするすべての第５のリンク情報付き役割識別子について、それぞれのリンク情報付き役割識別子の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第４のリンク情報付き役割識別子を所有者リンク情報付き役割識別子とするリンク指定型個別化アクセスチケットを新規生成

することを要旨とする。

【０１０６】

請求項４４記載の本発明にあっては、新規生成するリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子とするリンク情報付き役割識別子と、会員リンク情報付き役割識別子とするすべての第５のリンク情報付き役割識別子について、それぞれのリンク情報付き役割識別子の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第４のリンク情報付き役割識別子を所有者リンク情報付き役割識別子とするリンク指定型個別化アクセスチケットを新規生成する。

【０１０７】

更に、請求項４５記載の本発明は、通信網においてユーザ個人を隠蔽した通信を制御可能とする通信網であって、ユーザの特性を識別する付与情報をユーザに付与する第１の機関と、前記付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定する第２の機関と、アクセス権を示すリンク指定型個別化アクセスチケットを発行する第３の機関と、発信者からの発信要求に対して前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う第４の機関とを有することを要旨とする。

【０１０８】

請求項４５記載の本発明にあっては、付与情報をユーザに付与し、付与情報とユーザに関する情報とを対にして他のユーザからの閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示すリンク指定型個別化アクセスチケットを発行し、発信者からの発信要求に対してリンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う。

【０１０９】

請求項４６記載の本発明は、請求項４５記載の発明において、前記第１の機関の付与情報がリンク情報付き役割識別子であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、前記リン

ク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型１対１個別化アクセスチケットであり、前記第４の機関は発信者からの接続要求を、前記リンク情報付き役割識別子、前記リンク指定型１対１個別化アクセスチケット、および前記リンク指定型１対１個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対１個別化アクセスチケットが改竄されていないことを、発信者リンク情報付き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを要旨とする。

【０１１０】

請求項４６記載の本発明にあっては、第１の機関の付与情報はリンク情報付き役割識別子であり、発信者の指定情報は発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、リンク指定型個別化アクセスチケットは発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、有効期限を含むリンク指定型１対１であり、役割リンク情報付き識別子、リンク指定型１対１個別化アクセスチケット、リンク指定型１対１個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【０１１１】

また、請求項４７記載の本発明は、請求項４５記載の発明において、前記第１の機関の付与情報が発信者リンク情報付き役割識別子と個別化アクセスチケット

変更権(Enabler）であり、前記発信者の指定情報が所有者リンク情報付き役割識別子と１個以上の着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが所有者リンク情報付き役割識別子のリンク情報、１個以上の会員リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク１対Ｎ個別化アクセスチケットであり、第４の機関は発信者からの接続要求を、前記発信者リンク情報付き役割識別子、前記リンク指定型１対Ｎ個別化アクセスチケット、および前記リンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、第４の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを要旨とする。

【０１１２】

請求項４７記載の本発明にあっては、第１の機関の付与情報は発信者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler）であり、発信者の指定情報は発信者リンク情報付き役割識別子と１個以上の着信者リンク情報付き役割識別子であり、リンク指定型個別化アクセスチケットは所有者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ個別化アクセスチケットであり、発信者リンク情報付き役割識別子、リンク指定型１対Ｎ個別化アクセスチケット、リンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【０１１３】

更に、請求項４８記載の本発明は、請求項４５または４６または４７記載の発明において、前記第４の機関が、前記リンク指定型個別化アクセスチケットに関する第４の機関の認証結果が正しくても、着信者が第４の機関の着信拒否リストに該リンク指定型個別化アクセスチケットを登録している場合は、第４の機関は当該接続要求を拒否する拒否手段を有することを要旨とする。

【０１１４】

請求項４８記載の本発明にあっては、リンク指定型個別化アクセスチケットに関する認証結果が正しくても、着信者が着信拒否リストに該リンク指定型個別化アクセスチケットを登録している場合は、当該接続要求を拒否する。

【０１１５】

請求項４９記載の本発明は、アクセス権を示す情報であるリンク指定型個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法を実施するプログラムを記録した記録媒体であって、前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する接続制御プログラムを記録媒体に記録することを要旨とする。

【０１１６】

請求項４９記載の本発明にあっては、リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【０１１７】

また、請求項５０記載の本発明は、請求項４９記載の発明において、前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型１対１個別化アクセスチケットであり、リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク情報付き１対１個別化アクセスチケットが有効期限

内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録することを要旨とする。

【０１１８】

請求項５０記載の本発明にあっては、リンク指定型個別化アクセスチケットは発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、有効期限を含むリンク指定型１対１個別化アクセスチケットであり、リンク指定型１対１個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対１個別化アクセスチケットに含まれていること、およびリンク指定型１対１個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【０１１９】

更に、請求項５１記載の本発明は、請求項４９記載の発明において、前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ個別化アクセスチケットであり、第４の機関が発信者からの接続要求を、発信者リンク情報付き役割識別子、１個以上の着信者リンク情報付き役割識別子、リンク指定型１対Ｎ個別化アクセスチケット、およびリンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子が個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録することを要旨とする。

【０１２０】

請求項５１記載の本発明にあっては、リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index 、所有者Index 、移転制御情報、および有効期限情報を含むリンク指定型１対Ｎ所有者役割識別子であり、発信者リンク情報付き役割識別子、１個以上の着信者リンク情報付き役割識別子、リンク指定型１対Ｎ個別化アクセスチケット、リンク指定型１対Ｎ個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型１対Ｎ個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型１対Ｎ個別化アクセスチケットに含まれていること、およびリンク指定型１対Ｎ個別化アクセスチケットが有効期限内であることの３要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求に対してユーザ間の接続を行う接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【０１２１】

請求項５２記載の本発明は、請求項４９記載の発明において、前記検証結果が正しくても、リンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する接続制御プログラムを記録媒体に記録することを要旨とする。

【０１２２】

請求項５２記載の本発明にあっては、検証結果が正しくてもリンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【０１２３】

また、請求項５３記載の本発明は、個別化アクセスチケット変更権(Enabler)により第３の機関において所有者を変更する方法を実施するプログラムを記録した記録媒体であって、第１のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第１の個別化アクセスチケット変更権(Enabler) で照合

し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler) および第１のリンク情報付き役割識別子により新たに発信者リンク情報付き役割識別子を変更し、第３のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【０１２４】

請求項５３記載の本発明にあっては、第１のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第１の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler) および第１のリンク情報付き役割識別子により新たな発信者リンク情報付き役割識別子を変更し、第３のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【０１２５】

更に、請求項５４記載の本発明は、個別化アクセスチケット変更権(Enabler) により第３の機関において会員を追加する方法を実施するプログラムを記録した記録媒体であって、第４のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第３の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、１個以上の第４の個別化アクセスチケット変更権(Enabler) 、１個以上の第２のリンク情報付き役割識別子により１個以上の新たな着信者リンク情報付き役割識別子に追加し、第５のリンク情報付き個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【０１２６】

請求項５４記載の本発明にあっては、第４のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第３の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、１個以上の第４の個別化アクセスチケット変更権(Enabler) 、１個以上の第２のリンク情報付き役割識別子により１個以上の新たな着信者リンク情報付き役割識別子に追加し、第５のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【０１２７】

請求項５５記載の本発明は、個別化アクセスチケット変更権(Enabler) により第３の機関において会員を削除する方法を実施するプログラムを記録した記録媒体であって、第６のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第４の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、１個以上の第５の個別化アクセスチケット変更権(Enabler) 、１個以上の第３のリンク情報付き役割識別子により１個以上の着信者リンク情報付き役割識別子を削除し、第７のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【０１２８】

請求項５５記載の本発明にあっては、第６のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第４の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、１個以上の第５の個別化アクセスチケット変更権(Enabler) 、１個以上の第３のリンク情報付き役割識別子により１個以上の着信者リンク情報付き役割識別子を削除し、第７のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【０１２９】

また、請求項５６記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、リンク指定型個別化アクセスチケットが、発信者フラグ、移転制御フラグ、発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、有効期限、および第３の機関の秘密鍵による署名から構成されるリンク指定型１対１個別化アクセスチケットであり、リンク情報付き役割識別子が、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、リンク情報および第１の機関の秘密鍵による署名から構成され、個人識別子が、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、発信者と着信者の１対１対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【０１３０】

請求項５６記載の本発明にあっては、発信フラグ、移転制御フラグ、発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、有効期限、および第３の機関の秘密鍵による署名から構成されるリンク指定型１対１個別化アクセスチケットを発信者と着信者の１対１対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【０１３１】

更に、請求項５７記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、リンク指定型個別化アクセスチケットが、発信者Index 、所有者Index 、移転制御情報、発信者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、および有効期限情報から構成されるリンク指定型１対Ｎ個別化アクセスチケットであり、リンク情報付き役割識別子が、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、リンク情報、および第１の機関の秘密鍵による署名から構成され、個人識別子が、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【０１３２】

請求項５７記載の本発明にあっては、発信者Index 、所有者Index 、移転制御情報、発信者リンク情報付き役割識別子のリンク情報、１個以上の着信者リンク情報付き役割識別子のリンク情報、および有効期限情報から構成されるリンク情報付き１対Ｎ個別化アクセスチケットを発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【０１３３】

請求項５８記載の本発明は、個別化アクセスチケット変更権(Enabler) を記録したコンピュータで読み取り可能な記録媒体であって、個別化アクセスチケット

変更権(Enabler) が、個別化アクセスチケット変更権(Enabler) であることを一意に表す文字列、役割識別子、および第１の機関の秘密鍵による署名から構成され、リンク情報付き役割識別子が、個人識別子、暗号化された位置情報、第４の機関のホスト個人情報、リンク情報、および第１の機関の秘密鍵による署名から構成され、個人識別子が、第１の機関が一意に付与した文字列、および第１の機関の秘密鍵による署名から構成され、発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【０１３４】

請求項５８記載の本発明にあっては、個別化アクセスチケット変更権(Enabler) であることを一意に表す文字列、役割識別子、および第１の機関の秘密鍵による署名から構成される個別化アクセスチケット変更権(Enabler) を発信者と着信者の１対Ｎ対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【０１３５】

また、請求項５９記載の本発明は、リンク指定型個別化アクセスチケット（ＰＡＴ）の新規生成および既存のリンク指定型個別化アクセスチケット（ＰＡＴ）の内容変更を行うため、Ｎｕｌｌ－ＡＩＤ（AID_{Null}）および該Ｎｕｌｌ－ＡＩＤの Enabler(Enabler of Ｎｕｌｌ－ＡＩＤまたは Enabler of AID_{Null}) を使用し、該Ｎｕｌｌ－ＡＩＤを含む演算は、

(a) リンク指定型個別化アクセスチケット（ＰＡＴ）に対する新規生成（Make ＰＡＴ）、マージ（Merge ＰＡＴ）、分割（Split ＰＡＴ）、変更（Trans ＰＡＴ）からなる演算規則に従い、

(b) Ｎｕｌｌ－ＡＩＤにのみ適用可能な規則として、

ｉ．Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知であり、

ii. Enabler of Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知である

ことを要旨とする。

【０１３６】

請求項５９記載の本発明にあっては、リンク指定型個別化アクセスチケット（ＰＡＴ）の新規生成および既存のリンク指定型個別化アクセスチケット（ＰＡＴ）の内容変更を行うために、Ｎｕｌｌ－ＡＩＤ（AID_{Null}）および該Ｎｕｌｌ－ＡＩＤの Enabler(Enabler of Ｎｕｌｌ－ＡＩＤまたは Enabler of AID_{Null}）を使用するため、会員ＡＩＤおよびEnablerr of 会員ＡＩＤを所有者ＡＩＤに渡さなくても新規生成（MakeＰＡＴ）およびマージ（Merge ＰＡＴ）を行うことができる。

【０１３７】

更に、請求項６０記載の本発明は、請求項５９記載の発明において、前記Ｎｕｌｌ－ＡＩＤは、リンク指定型個別化アクセスチケット（ＰＡＴ）の所有者ＡＩＤとしてのみ使用可能であり、

【数１２】

$PAT<AID_{Null} \mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

は許可することを要旨とする。

【０１３８】

請求項６０記載の本発明にあっては、Ｎｕｌｌ－ＡＩＤはリンク指定型個別化アクセスチケット（ＰＡＴ）の所有者ＡＩＤとしてのみ使用可能であり、

【数１３】

$PAT<AID_{Null} \mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

は許可するため、$PAT<AID_{所有者} \mid AID_{会員}>$の所有者が$AID_{会員}$の Enabler を知らない場合には、このＰＡＴからＰＡＴ$<AID_{Null} \mid AID_{会員}>$を作成することはできない。

【０１３９】

請求項６１記載の本発明は、Ｇｏｄ－ＡＩＤ（AID_{God}）を用いて、リンク指定型個別化アクセスチケット（ＰＡＴ）に読取専用属性を設定し、該Ｇｏｄ－ＡＩＤに関する演算は、

(a) Ｇｏｄ－ＡＩＤは、すべてのユーザに既知であり、

(b) Ｇｏｄ－ＡＩＤに関する演算が、

【数１４】

ｉ．$AID_{所有者}$がAID_{Null}でもAID_{God}でもない場合：

$PAT<AID_{所有者}|AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

＋ Enabler of $AID_{所有者}$

$\rightarrow PAT<AID_{God}|AID_{所有者}, AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

ii．$AID_{所有者}$がAID_{Null}の場合：

$PAT<AID_{Null}|AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

＋ Enabler of AID_{Null}

$\rightarrow PAT<AID_{God}|AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$

である場合のいずれかのみ許可されることを要旨とする。

【０１４０】

請求項６１記載の本発明にあっては、Ｇｏｄ－ＡＩＤ（AID_{God}）を用いて、リンク指定型個別化アクセスチケット（ＰＡＴ）に読取専用属性を設定するため、グループ通信において参加者を固定することができる。

【０１４１】

また、請求項６２記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、Ｎｕｌｌ－ＡＩＤが、Ｎｕｌｌ－ＡＩＤであることを表す文字列および該文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【０１４２】

請求項６２記載の本発明にあっては、Ｎｕｌｌ－ＡＩＤであることを表す文字列および該文字列に対して認証局の署名を施したものからなるデータ構造のＮｕｌｌ－ＡＩＤを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【０１４３】

更に、請求項６３記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、 Enabler of Ｎｕｌｌ－ＡＩＤが、Enabler であることを表す文字列、Ｎｕｌｌ－ＡＩＤの実体、および前記Enabler であることを表す文字列と前記Ｎｕｌｌ－ＡＩＤの実体を連結した文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【０１４４】

請求項６３記載の本発明にあっては、Enabler であることを表す文字列、Ｎｕｌｌ－ＡＩＤの実体、およびEnabler であることを表す文字列とＮｕｌｌ－ＡＩＤの実体を連結した文字列に対して認証局の署名を施したものからなるデータ構造の Ehabler of Ｎｕｌｌ－ＡＩＤを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【０１４５】

請求項６４記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、Ｇｏｄ－ＡＩＤが、Ｇｏｄ－ＡＩＤであることを表す文字列および前記Ｇｏｄ－ＡＩＤであることを表す文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【０１４６】

請求項６４記載の本発明にあっては、Ｇｏｄ－ＡＩＤであることを表す文字列およびＧｏｄ－ＡＩＤであることを表す文字列に対して認証局の署名を施したものからなるデータ構造のＧｏｄ－ＡＩＤを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【０１４７】

【発明の実施の形態】

以下、図面を用いて本発明の第１の実施の形態について説明する。本発明の接続制御方法は、通信網における発信者および着信者の匿名性を保持しつつ、発信者からの通信をも適宜可能とするものであり、基本的には着信者の本当の識別子

を隠蔽した状態で、着信者の特性を表す情報のみを公開し、この公開された情報に基づいて、匿名性を保持したまま通信を希望する者に対して限定的なアクセス権を付与することにある。

【０１４８】

具体的には、図１（ａ）に示すように、ユーザに対して個人情報を隠蔽した役割識別子（Anonymous Identification：ＡＩＤと略称する）を付与し、この役割識別子ＡＩＤをユーザの特性を表す情報である趣味、年齢、職業等のようなユーザをネットワーク上で特定はできないが、発信者にとって当該ユーザと通信する価値があるかどうかを判断するための有用な情報と組にしてネットワークに公開する。

【０１４９】

また、発信者は、前記公開された情報を閲覧または検索することにより自分が通信したい相手を捜すことができる。すなわち、発信者が発信者自身の匿名性を保持したままある相手と通信したい場合には、その相手の役割識別子を指定し、個別化アクセスチケットＰＡＴ（Personalized Access Ticket）を取得する。

【０１５０】

個別化アクセスチケットＰＡＴには、後述する図３（ｃ）に示すように、発信者、着信者それぞれの役割識別子ＡＩＤの他に、発信者フラグ、移転制御フラグ、および、有効期限の各情報が記載されている。移転制御フラグは、図１（ｂ），（ｃ）に示すように着信拒否等の接続制御を行うために使用される。すなわち、移転制御フラグを立てると、後述するセキュア・コミュニケーション・サービスＳＣＳ（Secure Communication Service）は、接続要求の際に、発信者に対し、例えば署名の検証、パスワード要求等の認証を行う。また、移転制御フラグを立てない場合には、セキュア・コミュニケーション・サービスＳＣＳは認証無しで接続要求をセキュア・コミュニケーション・サービスＳＣＳが接続している物理的通信網に渡す。すなわち、移転制御は役割識別子ＡＩＤがこれを認証局ＣＡ（Certification Authority）から割り当てられたユーザによって正当に利用されているかを認証するために用いられる。

【０１５１】

本発明の接続制御方法を実施する通信網においては、ユーザに対する役割識別子ＡＩＤの付与、役割識別子ＡＩＤと組み合わされた情報の保持、個別化アクセスチケットＰＡＴの発行、および個別化アクセスチケットＰＡＴに基づく接続制御はそれぞれ別の機関で行われている。これは、それぞれの行為に関して保持すべきセキュリティレベルに差があるので、別々の機関で実行した方がネットワーク全体のセキュリティの保持には好都合だからである。

【０１５２】

図２は、本発明の一実施形態の全体構成図である。本実施形態はインターネット電子メールシステムを対象としたものである。図２において、１は認証局ＣＡであり、認証権限と役割識別子ＡＩＤの発行権限を有し、ユーザに対して役割識別子を割り当てる機能を有する。３はユーザであり、５はセキュア・コミュニケーション・サービスＳＣＳであり、ユーザ３間の電子メールを転送し、必要に応じて着信拒否および個人識別子の同一性を判定し、取り出す。７はアノニマス・ディレクトリ・サービスＡＤＳであり、役割識別子ＡＩＤ、移転制御情報、有効期限、および、プライバシー情報を管理するデータベースである。すなわち、アノニマス・ディレクトリ・サービスＡＤＳ７は、検索者の役割識別子ＡＩＤと検索条件（一般に、プライバシー情報）にマッチした登録者の役割識別子ＡＩＤから個別化アクセスチケットＰＡＴを発行し、検索者に交付する機能を有する。

【０１５３】

まず、ユーザの要求に基づいて個人識別子から役割識別子ＡＩＤを生成し、そのユーザに割り当てるまでの一連の処理について説明する。

【０１５４】

図３は、個人識別子ＯＩＤ(Official Identification)、役割識別子ＡＩＤおよび個別化アクセスチケットＰＡＴの例を示している。同図に示すように、個人識別子ＯＩＤは、図３（ａ）に示すように認証局ＣＡ１がユーザに一意に生成した任意の文字列に対して認証局ＣＡ１が秘密鍵で電子署名したものである。また、役割識別子ＡＩＤは、図３（ｂ）に示すように個人識別子ＯＩＤの一部とその位置情報、冗長な文字列、ＳＣＳのホストＯＩＤからなる文字列に対し、認証局

ＣＡ１の秘密鍵で電子署名を施したものである。

【０１５５】

また、個別化アクセスチケットＰＡＴは、図３（ｃ）に示すように、発信者フラグ、移転制御フラグ、役割識別子$ＡＩＤ_0$、役割識別子$ＡＩＤ_1$、有効期限からなる文字列に対してアノニマス・ディレクトリ・サービスＡＤＳのＯＩＤ秘密鍵による電子署名を施したものである。なお、この個別化アクセスチケットを以下１対１個別化アクセスチケットと称することにする。

【０１５６】

更に、後述する各実施形態で説明するように、本発明は、個別化アクセスチケットＰＡＴとして、上述した１対１個別化アクセスチケットに加えて、発信者と着信者を１対Ｎに対応させている１対Ｎ個別化アクセスチケット、および役割識別子の実体を個別化アクセスチケットで指定する代わりに役割識別子を指定するリンク情報を持ち、このリンク情報で役割識別子を指定するリンク指定指定型個別化アクセスチケットを有し、このリンク指定型個別化アクセスチケットには上述した発信者と着信者の対応関係に基づきリンク指定型１対１個別化アクセスチケットとリンク指定型１対Ｎ個別化アクセスチケットがある。すなわち、本発明の個別化アクセスチケットには、１対１個別化アクセスチケット、１対Ｎ個別化アクセスチケット、リンク指定型１対１個別化アクセスチケット、およびリンク指定型１対Ｎ個別化アクセスチケットの４種類がある。

【０１５７】

次に、ユーザ３が役割識別子ＡＩＤを認証局ＣＡ１に対して請求する処理について図４に示すフローチャートを参照して説明する。ユーザは個人識別子ＯＩＤと請求項目を入力して（ステップＳ４１１）、図７に示すようにＡＩＤ請求メッセージを作成し（ステップＳ４１３）、ユーザＯＩＤの秘密鍵で署名、暗号化し（ステップＳ４１５）、それから該ＡＩＤ請求メッセージを認証局ＣＡ１に電子メールで送信する（ステップＳ１４７）。

【０１５８】

ＡＩＤ請求メッセージは、発信者の個人識別子ＯＩＤと請求項目から構成され、請求項目は次に示す２種類のうちのいずれかである。

【０１５９】

(1) 新規な役割識別子ＡＩＤの割り当てを要求する場合：

REQUEST AID ＜要求するＡＩＤの数＞

(2) 既存の役割識別子ＡＩＤの廃止を要求する場合：

DISCARD AID ＜廃止したいＡＩＤの実体＞

次に、上述した役割識別子ＡＩＤの請求に対する認証局ＣＡ１が役割識別子ＡＩＤをユーザ３に対して交付する処理について図５に示すフローチャートを参照して説明する。図５において、認証局ＣＡ１は、ユーザ３からの上述したＡＩＤ請求メッセージを受信すると（ステップＳ５１１）、認証局ＣＡ１はユーザ３のＯＩＤ公開鍵を用いてＡＩＤ請求メッセージ（図７）を復号化、認証する（ステップＳ５１３）。認証局ＣＡ１は該メッセージが改竄されているか否かをチェックする（ステップＳ５１５）。改竄を検出した場合には、該メッセージを破棄するが、改竄が認められなかった場合には、認証局ＣＡ１は役割識別子ＡＩＤを生成し（ステップＳ５１７）、ＡＩＤ秘密鍵およびＡＩＤ公開鍵を生成し（ステップＳ５１９）、図８に示すＡＩＤ交付メッセージを生成する（ステップＳ５２１）。それから、認証局ＣＡ１は該メッセージをユーザＯＩＤの公開鍵で署名、暗号化し（ステップＳ５２３）、この署名したメッセージをユーザ３のＯＩＤに送信する（ステップＳ５２５）。

【０１６０】

次に、図６に示すフローチャートを参照して、ユーザにおけるＡＩＤ交付処理について説明する。図６において、ユーザ３が認証局ＣＡ１からの暗号化されたＡＩＤ交付メッセージを受信すると（ステップＳ６１１）、ユーザ３はユーザ秘密鍵を用いてＡＩＤ交付メッセージを復号化、認証し（ステップＳ６１３）、該メッセージが改竄されているか否かをチェックする（ステップＳ６１５）。改竄を検出した場合には、エラーメッセージを出力し、該ＡＩＤ交付メッセージを破棄する（ステップＳ６１７）。また、改竄が認められない場合には、ＡＩＤ交付メッセージから役割識別子ＡＩＤとＡＩＤ秘密鍵を抽出し、ユーザ３に通知する（ステップＳ６１９）。

【０１６１】

ＡＩＤ交付メッセージは、図８に示すように発信者ＯＩＤと処理結果から構成されている。処理結果は次に示す２種類のうちのいずれかである。

【０１６２】

(1) 新規な役割識別子ＡＩＤの交付の場合：

NEW AID ＜新規ＡＩＤの実体とＡＩＤの秘密鍵｜ＡＩＤ取得失敗＞

(2) 既存の役割識別子ＡＩＤの廃止

DISCARD AID ＜既存ＡＩＤの実体＞＜廃止完了｜廃止失敗＞

次に、認証局ＣＡにおける役割識別子ＡＩＤの生成処理について図９、図１０を参照して説明する。図９において、認証局ＣＡ１は乱数発生等の任意の手段を用いて、個人識別子ＯＩＤの全長Ｌと等しい長さの文字列を生成し、この文字列を仮の役割識別子ＡＩＤとして生成する（ステップＳ９１１）。

【０１６３】

次に、個人識別子ＯＩＤの複写を行うために、個人識別子ＯＩＤのコピー範囲を指定するｐとｌの値を決定する（ステップＳ９１３）。これは、乱数発生等の任意の手段を用いて、パラメータp_iとl_iの値をそれぞれ$0 \leqq p_i \leqq L$および$l_{min} \leqq l_i \leqq l_{Max}$のようにコピー範囲を決定する。ここで、Ｌは個人識別子ＯＩＤの全長であり、l_{min}およびl_{Max}は$0 < l_{min} < l_{Max} < L$が成り立つ範囲で任意に定めた値とする。それから、コピー先頭位置を個人識別子ＯＩＤの先頭から距離p_iに設定し、終端位置を$p_i + l_i$に設定するというようにコピー範囲を設定する。次に、図１０（ａ），（ｂ）に示すように、ペースト先頭位置を仮の役割識別子ＡＩＤの先頭から距離p_iに設定し、終端位置を$p_i + l_i$に設定するというようにペースト位置を設定する。

【０１６４】

それから、図１０（ａ），（ｂ）に示すように、上述したコピー範囲の文字列を仮の役割識別子ＡＩＤの上述したペースト位置に上書きして複写する（ステップＳ９１５）。このように上書きした文字列の特定の位置に位置情報p_iおよびl_iの値を、ＣＡが定めた方法で暗号化して、図１０（ｃ）で指定した位置に付加し（ステップＳ９１７）、更にこの位置情報を付加した文字列にセキュア・コ

ミュニケーション・サービスＳＣＳのホストＯＩＤ（ホスト名、ドメイン名、またはＩＰアドレス）を図１０（ｃ）に示すように付加する（ステップＳ９１９）。そして、このようにセキュア・コミュニケーション・サービスＳＣＳのホストＯＩＤを付加した文字列に認証局ＣＡのＯＩＤ秘密鍵で電子署名を施す（ステップＳ９２１）。

【０１６５】

次に、役割識別子ＡＩＤによる個人情報の登録および検索について説明する。アノニマス・ディレクトリ・サービスＡＤＳ７において、個人情報を登録するまでの流れを図１１（ａ）に示す。同図に示すように、登録者であるユーザＢ３は自らの役割識別子ＡＩＤ、移転制御情報、有効期限、および、性別、年齢、趣味等のプライバシー情報をアノニマス・ディレクトリ・サービスＡＤＳ７に送付する。

【０１６６】

また、アノニマス・ディレクトリ・サービスＡＤＳ７における検索処理を図１１（ｂ）に示す。検索者であるユーザＡ３は、自らの役割識別子ＡＩＤと例えば性別、年齢、趣味といったプライバシー情報からなる検索条件をアノニマス・ディレクトリ・サービスＡＤＳ７に送信する。アノニマス・ディレクトリ・サービスＡＤＳ７は、これらの情報を受信すると、検索条件にマッチした登録者の役割識別子ＡＩＤを抽出する。アノニマス・ディレクトリ・サービスＡＤＳ７は最後に検索者の役割識別子ＡＩＤと検索条件にマッチした登録者の役割識別子ＡＩＤから個別化アクセスチケットＰＡＴを生成し、検索者であるユーザＡ３に交付する。

【０１６７】

１対１個別化アクセスチケットの生成は、アノニマス・ディレクトリ・サービスＡＤＳ７の検索結果として生成する。

【０１６８】

次に、図１２のフローチャートを参照して、ＡＤＳにおけるＰＡＴ生成処理について説明する。

【０１６９】

１．検索者ＡＩＤ秘密鍵で署名された検索者ＡＩＤを入力する（ステップＳ１２１０）。

２．ステップＳ１２１０における検索者ＡＩＤをその検索者ＡＩＤの公開鍵で認証する（ステップＳ１２１１）。

【０１７０】

３．ステップＳ１２１１における認証の結果

・検索者ＡＩＤが改竄されている場合処理を中止する。

・検索者ＡＩＤが改竄されていない場合、ステップＳ１２１５に進む。

４．ステップＳ１２１１で認証済みの検索者ＡＩＤを、登録者ＡＩＤ（ＡＤＳ登録時に登録者ＡＩＤの秘密鍵で認証済み）と連結する（ステップＳ１２１５）。

５．ステップＳ１２１５で連結した、検索者ＡＩＤと登録者ＡＩＤからなる文字列に、登録者によりあらかじめ設定された移動制御フラグと有効期限を設定する。また、発信者フラグを「０」と設定する（ステップＳ１２１７）。

６．ステップＳ１２１７の結果に、ＡＤＳのＯＩＤ秘密鍵で署名する（ステップＳ１２１９）。

７．ステップＳ１２１９の結果（つまり、ＰＡＴ）を、検索者ＡＩＤに送信する（ステップＳ１２２１）。

なお、ＰＡＴを受信した検索者は、ＡＤＳのＯＩＤ公開鍵を用いて受信したＰＡＴを認証し、改竄されていなければ、これを検索者端末の記憶装置に記憶し、改竄されていれば、破棄します。この手順は、図６と同様である。

【０１７１】

次に、１対１個別化アクセスチケットＰＡＴによる移転制御について説明する。移転制御は、発信者番号通知のために行われるが、この発信者番号通知とは、着信者が発信者の役割識別子ＡＩＤと実際の発信者を対応付けられるようにすることである。

【０１７２】

アノニマス・ディレクトリ・サービスＡＤＳ７および着信者は、個別化アクセスチケットＰＡＴの移転制御フラグを設定することにより、発信者に番号通知さ

せるか否かを選択させることができる。

【０１７３】

移転制御フラグを「１」に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５で移転制御が行われるため、着信者は発信者の役割識別子ＡＩＤと実際の発信者を対応付けることができる（発信者番号通知）。また、移転制御フラグを「０」に設定した場合には、着信者は発信者の役割識別子ＡＩＤと実際の発信者を対応付けることができない（発信者番号非通知）。

【０１７４】

図１４のフローチャートを参照して、ＳＣＳにおけるメール接続制御の処理手順について説明する。

【０１７５】

１．メールを入力する（ステップＳ１４１１）。

２．ステップＳ１４１１のメールのＴｏ：フィールドからＰＡＴを抽出する。次に、このＰＡＴに対するＡＤＳ公開鍵をＡＤＳに何らかの手段で問い合わせ、そのＡＤＳ公開鍵を取得する。そして、ＰＡＴをＡＤＳ公開鍵で認証する（ステップＳ１４１３）。

【０１７６】

３．ステップＳ１４１３における認証の結果

・ＰＡＴが改竄されている場合、ステップＳ１４１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する（ステップＳ１４２９）。

・ＰＡＴが改竄されていない場合、ステップＳ１４１７に進む。

４．ステップＳ１４１１のメールのＦｒｏｍ：フィールドから発信者ＡＩＤを抽出する。また、メールのＴｏ：フィールドのＰＡＴの移転制御フラグを解析し、ＰＡＴから発信者ＡＩＤを抽出する（ステップＳ１４１７，Ｓ１４１９）。

５．ステップＳ１４１７，Ｓ１４１９で抽出した発信者ＡＩＤ同士を比較する（ステップＳ１４２１）。

【０１７７】

６．ステップＳ１４２１における比較の結果

・両者が一致しない場合ステップＳ１４１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する（ステップＳ１４２９）。

・両者が一致する場合、ステップＳ１４２５に進む。

７．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴから有効期限を抽出する（ステップＳ１４２５）。

８．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴが有効期限内かどうかを検証する（ステップＳ１４２７）。

９．ステップＳ１４２７における検証の結果

・有効期限を過ぎている場合、ステップＳ１４１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する（ステップＳ１４２９）。

・有効期限内の場合、ステップＳ１４３１に進む。

１０．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴから移転制御フラグ値を調べる。

１１．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴから移転制御フラグ値を抽出する（ステップＳ１４３１）。

【０１７８】

１２．ステップＳ１４３１における抽出の結果

・移転制御フラグ値が「１」の場合、図１５～図１７の手順に従い、移転制御を行ってから（ステップＳ１４３５）、図１８の手順に従い、メールを着信者ＡＩＤ宛に転送する（ステップＳ１４３７）。

・移転制御フラグ値が「０」の場合、図１８の手順に従い、メールを着信者ＡＩＤ宛に転送する（ステップＳ１４３７）。

この移転制御について図１５～図１７を参照して説明する。まず、図１５において、セキュア・コミュニケーション・サービスＳＣＳ５は、個別化アクセスチケットＰＡＴを入力すると（ステップＳ１５１１）、それから、セキュア・コミュニケーション・サービスＳＣＳ５は、任意の文字列、例えばタイムスタンプを生成し（ステップＳ１５１７）、この生成した文字列を発信者の役割識別子ＡＩ

Ｄに送信する（ステップＳ１５１９）。

【０１７９】

ユーザにおいては、図１６に示すように、前記文字列を受信すると（ステップＳ１６１１）、この文字列に発信者役割識別子ＡＩＤの秘密鍵で署名し（ステップＳ１６１３）、署名つき該文字列をセキュア・コミュニケーション・サービスＳＣＳ５に送信する（ステップＳ１６１５）。

【０１８０】

セキュア・コミュニケーション・サービスＳＣＳ５においては、図１７に示すように、署名つき前記文字列を受信すると（ステップＳ１７１１）、発信者の役割識別子ＡＩＤの公開鍵で認証し（ステップＳ１７１３）、改竄されているか否かをチェックする（ステップＳ１７１５）。改竄されている場合には、改竄されている旨を何らかの手段で発信者ＡＩＤに通知してからアボート（異常終了）するが（ステップＳ１７１７）、改竄されていない場合には、セキュア・コミュニケーション・サービスＳＣＳ５は、図１８に示す接続制御を行う。

【０１８１】

以下、図１８のフローチャートを参照して接続制御について説明する。

【０１８２】

１．メールのＴｏ：フィールドのＰＡＴから、発信者のＳＣＳホストＯＩＤと着信者のＳＣＳホストＯＩＤを抽出する（ステップＳ１８１１）。

２．ステップＳ１８１１で抽出した発信者、着信者それぞれのＳＣＳホストＯＩＤのデータ形式を調べる（ステップＳ１８１３）。

【０１８３】

３．ステップＳ１８１３における調査の結果

・発信者ＳＣＳホストＯＩＤと着信者ＳＣＳホストＯＩＤのうち、少なくとも一方がホスト名もしくはドメイン名で与えられている場合には、ステップＳ１８１５に進み、ホスト名またはドメイン名で与えられているＳＣＳホストＯＩＤをＤＮＳ(Domain Name Service) に問い合わせ、そのホスト名またはドメイン名に対するＩＰアドレスを取得してから、ステップＳ１８１７に進む。

【０１８４】

・発信者ＳＣＳホストＯＩＤと着信者ＳＣＳホストＯＩＤがともにＩＰアドレスで与えられている場合には、そのままステップＳ１８１７に進む。

４．ステップＳ１８１５，Ｓ１８１７で抽出あるいは変換したＩＰアドレスを比較する（ステップＳ１８１７）。

【０１８５】

５．ステップＳ１８１７における比較の結果

・発信者ＳＣＳホストＯＩＤ（ＩＰアドレス）と着信者ＳＣＳホストＯＩＤ（ＩＰアドレス）が一致する場合、ステップＳ１８１９からステップＳ１８２３に進み、発信者ＡＩＤをアカウントに持つＳＣＳホスト上で、着信者ＡＩＤを検索する（ステップＳ１８２３）。この検索の結果、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在しない場合、ステップＳ１８２５からステップＳ１８２７に進み、ステップＳ１８１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【０１８６】

また、ステップＳ１８２５において、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在する場合、着信者ＡＩＤを検索条件として、着信拒否データベースに問い合わせる（ステップＳ１８２９）。

【０１８７】

この問い合わせの結果、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されている場合、ステップＳ１８３１からステップＳ１８２７に進み、メールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【０１８８】

また、ステップＳ１８３１において、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されていない場合、メールを、着信者のメールボックスまたはスプールに格納

して正常終了する（ステップＳ１８３３）。

【０１８９】

一方、ステップＳ１８１９において、発信者ＳＣＳホストＯＩＤ（ＩＰアドレス）と着信者ＳＣＳホストＯＩＤ（ＩＰアドレス）が一致しない場合、について説明する。

【０１９０】

まず、ＳＭＴＰに従い、メールを着信者ＡＩＤをアカウントに持つＳＣＳホストに転送する（ステップＳ１８３５）。

【０１９１】

次に、着信者ＡＩＤをアカウントに持つＳＣＳホスト上で、着信者ＡＩＤを検索する（ステップＳ１８３７）。

【０１９２】

この検索の結果、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在しない場合、ステップＳ１８３９からステップＳ１８４１に進み、メールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【０１９３】

また、ステップＳ１８３９において、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在する場合、ステップＳ１８４３に進む。ステップＳ１８４３では着信者ＡＩＤを検索条件として、着信拒否データベースに問い合わせる。

【０１９４】

ステップＳ１８４３における問い合わせの結果、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されている場合、ステップＳ１８４５からステップＳ１８４１に進み、メールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【０１９５】

また、ステップＳ１８４５において、メールのＴｏ：フィールドのＰＡＴ、ま

たは、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されていない場合、ステップＳ１８４７に進み、メールを、着信者のメールボックスまたはスプールに格納して正常終了する。

【０１９６】

図１９のフローチャートを参照して、ＳＣＳにおけるメール返信処理についてに説明する。

【０１９７】

１．エラーを検出したＳＣＳホストは、ＰＡＴ＜エラーを検出したＳＣＳホストＯＩＤ｜Ｆｒｏｍ：フィールドの発信者ＡＩＤ＞を生成する（ステップＳ１９１１）。

２．ステップＳ１９１１のＳＣＳホストは、ステップＳ１９１１で生成したＰＡＴを、エラーが発生したメールのＴｏ：フィールドにセットする（ステップＳ１９１３）。

３．ステップＳ１９１１のＳＣＳホストは、ステップＳ１９１３でセットしたメールを（発信者ＡＩＤ宛に）送信する（ステップＳ１９１５）。

【０１９８】

次に、個別化アクセスチケットＰＡＴに対する着信拒否について説明する。

【０１９９】

着信者ＡＩＤ側で指定した個別化アクセスチケットＰＡＴがＴｏ：フィールドに記述されたメールが、着信者ＡＩＤに含まれるホストＯＩＤのセキュア・コミュニケーション・サービスＳＣＳ５に到着した場合には、そのセキュア・コミュニケーション・サービスＳＣＳ５はそのメールを着信者のメールボックスまたはスプールには格納せず、発信者ＡＩＤ宛に返信する。この一連の処理を着信拒否と呼ぶ。

【０２００】

ユーザにおける着信拒否申請処理について図２２に示すフローチャートを参照して説明する。ユーザは役割識別子ＡＩＤと個別化アクセスチケットＰＡＴを入力し（ステップＳ２２１１）、図２４の上側に示す着信拒否申請メッセージを作成し（ステップＳ２２１３）、着信者ＡＩＤの秘密鍵で署名、暗号化する（ステ

ップＳ２２１５）。それから、着信者はこの暗号化した申請メッセージをセキュア・コミュニケーション・サービスＳＣＳ５に送信する（ステップＳ２２１７）。

【０２０１】

着信拒否申請メッセージは、図２４の上側に示すように、着信者の役割識別子ＡＩＤと申請項目から構成される。申請項目は次の２種類のうちのいずれかである。

【０２０２】

(1) 着信拒否の設定

＜着信者ＡＩＤの実体＞REFUSE＜ＰＡＴの実体、ＩＰアドレス、ドメイン名、ホスト名＞

(2) 着信拒否の解除

＜着信者ＡＩＤの実体＞RECONNECT ＜ＰＡＴの実体、ＩＰアドレス、ドメイン名、ホスト名＞

【０２０３】

次に、図２３に示すフローチャートを参照して、セキュア・コミュニケーション・サービスＳＣＳ５における着信拒否設定処理について説明する。セキュア・コミュニケーション・サービスＳＣＳ５は、着信拒否申請メッセージを受け取ると（ステップＳ２３１１）、着信者のＡＩＤ公開鍵で認証し（ステップＳ２３１３）、改竄されているか否かをチェックする（ステップＳ２３１５）。改竄されていない場合には、着信拒否メッセージから個別化アクセスチケットＰＡＴ、ＩＰアドレス、ドメイン名、またはホスト名を抽出し（ステップＳ２３１７）、該個別化アクセスチケットＰＡＴ、該ＩＰアドレス、該ドメイン名、該ホスト名を着信拒否データベース（ＤＢ）に登録（または削除）する（ステップＳ２３１９）。それから、図２４の下側に示すような着信拒否通知メッセージを生成し（ステップＳ２３２１）、着信者ＡＩＤ公開鍵で署名、暗号化し（ステップＳ２３２３）、この暗号化されたメッセージを着信者ＡＩＤに返信する（ステップＳ２３２５）。

【０２０４】

着信拒否通知メッセージは、図２４の下側に示すように、着信者の役割識別子ＡＩＤと処理結果から構成されている。処理結果は次に示す２種類のうちのいずれかである。

【０２０５】

(1) 着信拒否の設定結果

＜着信者ＡＩＤの実体＞REFUSE＜成功｜失敗＞＜ＰＡＴの実体、ＩＰアドレス、ドメイン名、ホスト名＞

(2) 着信拒否の解除結果

＜着信者ＡＩＤの実体＞RECONNECT ＜成功｜失敗＞＜ＰＡＴの実体、ＩＰアドレス、ドメイン名、ホスト名＞

着信拒否の実行に当たっては、セキュア・コミュニケーション・サービスＳＣＳ５は、個別化アクセスチケットＰＡＴを着信拒否データベースに問い合わせる。該当個別化アクセスチケットが存在する場合、または、発信者ＡＩＤに、該当するＩＰアドレス、ホスト名、ドメイン名が含まれる場合には、メールを発信者ＡＩＤに返信する。存在しない場合には、メッセージを着信者アカウントのメールボックスまたはスプールに格納する。

【０２０６】

図２５のフローチャートを参照して、同一性の判定について説明する。

【０２０７】

１．変数OID_Mの初期値を、ＯＩＤの全長Ｌと等しい長さで、かつ、すべての値が０であるビット列と定義する。また、変数OID_Vの初期値を、ＯＩＤの全長Ｌと等しい長さで、かつ、すべての値が０であるビット列と定義する（ステップＳ２５１１）。

【０２０８】

２．処理対象のＡＩＤの集合から１個のＡＩＤを選択し、以下のビット演算を実行する（ステップＳ２５１３）。

【０２０９】

(a) ＡＩＤに含まれる位置情報をもとにして、変数AID_Mと変数AID_Vの

値を決定する（ステップＳ２５１５）。ここで、

・AID_M はＯＩＤの全長Ｌと等しい長さで、かつ、

－ＯＩＤ情報が定義されている位置の値は１である。

－ＯＩＤ情報が定義されていない位置の値は０である。

ビット列と定義する（図２６）。

【０２１０】

・AID_V はＯＩＤの全長Ｌと等しい長さで、かつ、

－ＯＩＤ情報が定義されている位置の値はＯＩＤ情報の実際の値である

－ＯＩＤ情報が定義されていない位置の値は０である。

ビット列と定義する（図２６）。

【０２１１】

(b) OID_M とAID_M のＡＮＤ演算を実行し、その結果を変数OVR_M に代入する（ステップＳ２５１７）。

【０２１２】

(c) OVR_M とAID_M のＡＮＤ演算と、OVR_M とOID_M のＡＮＤ演算を実行し、その演算結果を比較する（ステップＳ２５１９）。

・一致する場合OID_M とAID_M のＯＲ演算を実行し、実行結果をOID_M に代入する（ステップＳ２５２１）。また、OID_V とAID_V のＯＲ演算を実行し、実行結果をOID_M に代入する（ステップＳ２５２３）。

・一致しない場合、ステップＳ２５２５に進み、実行する。

【０２１３】

(d) 処理対象のＡＩＤの集合から、次に処理するＡＩＤを抽出する。

・集合に少なくとも１個のＡＩＤが含まれている場合、ステップＳ２５１９を実行する。

・集合にＡＩＤが１個も含まれていない場合、ステップＳ２５２７に進む。

【０２１４】

(e) OID_M およびOID_V の値を出力する（ステップＳ２５２７）。

最終的に得られたOID_M の値は、処理対象のＡＩＤの集合から復元できたＯＩＤ情報のすべての位置を表している。また、最終的に得られたOID_V の値は

、処理対象のＡＩＤの集合から復元できたＯＩＤ情報のすべてを表している。つまり、OID_M とOID_V の値を用いると、

(a) OID_V の値を検索条件とすると、確率的にではあるがＯＩＤを求めることができる。

【０２１５】

(b) 上記検索の精度を、ＯＩＤ全長Ｌとの比OID_M Ｌで定量的に評価することができる。

【０２１６】

上述したように、本実施形態では、ユーザは、氏名、電話番号、電子メールアドレスといった情報を含む個人識別子ＯＩＤからこれらの情報を隠蔽した役割識別子ＡＩＤを作成すべく図７に示すような役割識別子ＡＩＤ請求メッセージを作成し、認証局ＣＡ１に送信すると、認証局ＣＡ１は、該メッセージを受け取って、役割識別子ＡＩＤを生成し、ユーザに交付する。

【０２１７】

ユーザは、この交付された役割識別子ＡＩＤおよび性別、年齢、趣味等の個人情報をアノニマス・ディレクトリ・サービスＡＤＳ７に送信し、アノニマス・ディレクトリ・サービスＡＤＳ７に役割識別子ＡＩＤと個人情報を登録する。このように登録された情報を検索する場合は、検索者は自己の役割識別子ＡＩＤと検索条件（性別、年齢、趣味等のプライバシー情報）をアノニマス・ディレクトリ・サービスＡＤＳ７に送信する。アノニマス・ディレクトリ・サービスＡＤＳ７は、これらの情報を受信すると、該検索条件にマッチした登録者の役割識別子ＡＩＤを抽出する。そして、アノニマス・ディレクトリ・サービスＡＤＳ７は、検索者の役割識別子ＡＩＤと検索条件にマッチした登録者の役割識別子ＡＩＤから１対１個別化アクセスチケットＰＡＴを生成し、検索者に交付する。

【０２１８】

この１対１個別化アクセスチケットＰＡＴには、図３（ｃ）に示すように発信者フラグ、移転制御フラグ、有効期限の値が設定されるが、この有効期限を着信者側で設定することにより、発信者からの接続を制限することができる。

【０２１９】

また、移転制御フラグの設定内容により発信者に番号通知させるか否かを、すなわち着信者が発信者ＡＩＤと実際の発信者を対応づけられるようにすることができるか否かを選択することができる。すなわち、移転制御フラグを１に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５で移転制御が行われ、着信者は発信者ＡＩＤと実際の発信者を対応付けることができる（発信者番号通知）。また、該フラグを０に設定した場合は、移転制御は行われず、着信者は発信者ＡＩＤと実際の発信者を対応付けることはできない（発信者番号非通知）。

【０２２０】

また、１対１個別化アクセスチケットＰＡＴで着信者を指定した呼を個別化アクセスチケットＰＡＴ内で定義した着信者役割識別子ＡＩＤまたは発信者役割識別子ＡＩＤに着信するように、通信網に対して接続要求をすることができる。更に、１対１個別化アクセスチケットＰＡＴで指定した呼のうち、着信者が選択した１対１個別化アクセスチケットＰＡＴの呼を着信拒否することができる。また更に、匿名性を悪用し複数の発信者役割識別子ＡＩＤで個人攻撃を繰り返す発信者への対処として、それら複数の発信者役割識別子ＡＩＤから個人識別子ＯＩＤの同一性を判定することができ、かつ、その個人識別子をある確率で取り出すことができる。

【０２２１】

次に、本発明の第２の実施形態に係る接続制御方法について図３１乃至図６０を参照して説明する。上述した第１の実施形態では発信者と着信者を１対１に対応させるとともに、偽装防止のためにユーザ要求に基づいた個別化アクセスチケットの新規生成、内容変更を許可していない場合について説明したのに対して、第２の実施形態では、発信者と着信者を１対Ｎに対応させるとともに、この１対Ｎ個別化アクセスチケットの新規生成、内容変更をユーザ主導で可能とする場合について説明するものである。なお、この発信者および着信者は所有者または会員である。

【０２２２】

一般に、グループ通信（メーリングリスト等）の会員構成は動的に変化するため、グループ通信の主催者は会員の電話番号、電子メールアドレス、インターネットメールアドレス等の連絡先情報を管理する必要がある。これに対して、第１の実施形態のように、個別化アクセスチケットの新規生成、内容変更ができない場合には、連絡先情報の管理が困難である。例えば、グループを一体として管理することが困難であり、また移転制御のため、他の人に渡しても、メーリングリスト等グループ通信のアドレスとして機能しない。

【０２２３】

本第２の実施形態では、このような不具合を解消するために１対Ｎ個別化アクセスチケットＰＡＴの新規生成および既存の１対Ｎ個別化アクセスチケットＰＡＴの内容変更をユーザ主導でできるようにしている。

【０２２４】

まず、本第２の実施形態で使用される各識別子の定義について図３１、図３２を参照して説明する。

【０２２５】

個人識別子（Official Identification ：ＯＩＤ）は、図３１（ａ）に示すように、認証局（Certificate Authority ：ＣＡ）が任意に生成した文字列（電話番号、電子メールアドレス等）、または前記文字列に対しＣＡ秘密鍵で電子署名を施したものである。

【０２２６】

役割識別子（Anonymous Identification：ＡＩＤ）は、図３１（ｂ）に示すように、ＯＩＤの一部分とその位置情報、任意に生成した冗長な文字列、ＳＣＳのホストＯＩＤからなる文字列に対し、ＣＡ秘密鍵で電子署名を施したものである。また、ＡＩＤはＳＣＳやＣＡで暗号化する場合もある。

【０２２７】

個別化アクセスチケット（Personalized Access Ticket：ＰＡＴ）は、図３１（ｃ）に示すように、１個の所有者ＡＩＤ（HolderＡＩＤ）、１個以上の会員ＡＩＤ（MemberＡＩＤ）、発信者インデックス、所有者インデックス、有効期限情

報、移転制御情報、ＰＡＴ演算装置識別子から構成されるリストに対し、ＰＡＴ演算装置識別子の秘密鍵で署名したものである。ここで、発信者インデックスは、ＡＩＤリスト中の発信者ＡＩＤの位置を表す数値データで、先頭ＡＩＤが発信者ＡＩＤであれば１、２番目ならば２，…、ｎ番目ならばｎである。所有者インデックスは、ＡＩＤリスト中の所有者ＡＩＤの位置を表す数値データで、先頭ＡＩＤが所有者ＡＩＤであれば１、２番目ならば２，…、ｎ番目ならばｎであると定義する。移転制御情報は、移転可の場合は「０」という数値、また移転不可の場合は「１」という数値のいずれかで表す。

【０２２８】

所有者ＡＩＤは、ＡＩＤリスト中の所有者インデックスで指定した位置に書き込まれているＡＩＤである。会員ＡＩＤは、所有者ＡＩＤ以外のすべてのＡＩＤである。有効期限情報は、数値データであって、使用可能回数、ＰＡＴが利用不可能になる絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になる絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になってから利用不可能になるまでの相対時間（寿命）のいずれか、または複数を組み合わせて記述する。ＰＡＴ演算装置識別子は、ＰＡＴ演算装置のシリアルナンバーである。ＰＡＴ演算装置の秘密鍵は、上記シリアルナンバーに対する秘密鍵である。これらの中で、所有者ＡＩＤと会員ＡＩＤからなる部分を以後、ＡＩＤリストと呼ぶことにする。

【０２２９】

また、本第２の実施形態では、所有者役割識別子ＡＩＤに対応した識別子として、Enabler を導入している。Enabler は、図３２に示すように、Enabler であることを通信網上で一意に表す文字列とＡＩＤからなる文字列に対して、ＣＡ秘密鍵で電子署名したものである。

【０２３０】

次にＰＡＴの新規生成および内容変更における操作について説明する。通信端末上のセキュアなＰＡＴ演算装置、ＣＡ上もしくはＣＡから正当に依頼されたネットワーク上のＰＡＴ演算オブジェクト（以後、これもＰＡＴ演算装置と呼ぶことにする）において、次の操作が定義される。

【０２３１】

(1) ＡＩＤリストの演算：

所有者ＡＩＤおよび所有者ＡＩＤに対応するEnabler を用いて、ＡＩＤリストを新規生成あるいは変更する。

(2) 有効期限情報および移転制御情報の設定：

所有者ＡＩＤおよび所有者ＡＩＤに対応するEnabler を用いて、有効期限情報および移転制御情報を設定もしくは変更する。

【０２３２】

所有者ＡＩＤに対してのみＡＩＤリストの演算を許可するために、以下の演算規則を定義する。

【０２３３】

(1) 新規生成（MakePＡＴ）（図３３参照）：

ＡＩＤリスト（ＡＬＩＳＴ＜所有者ＡＩＤ｜会員AID_1，会員AID_2，…，会員AID_n＞）を新規生成し、生成後のＡＬＩＳＴに対し、有効期限情報および移転制御情報を設定する。

【０２３４】

【数１５】

$$AID_A + AID_B + \text{Enabler of } AID_B + \text{Enabler of } AID_A$$
$$\rightarrow ALIST<AID_A \mid AID_B> ALIST<AID_A \mid AID_B>$$
$$+ \text{Enabler of } AID_A + \text{有効期限情報} + \text{移転制御情報}$$
$$\rightarrow PAT<AID_A \mid AID_B>$$

(2) マージ（Merge ＰＡＴ）（図３４参照）：

同一所有者ＡＩＤの複数ＡＬＩＳＴをマージし、マージ後のＡＬＩＴＳに対し、有効期限情報および移転制御情報を設定する。

【０２３５】

【数１６】

$$ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots>$$
$$+ ALIST<AID_A \mid AID_{C1}, AID_{C2}, \cdots>$$
$$+ \text{Enabler of } AID_A$$

$$\rightarrow ALIST<AID_A \mid AID_{B1},\ AID_{B2},\ \cdots,\ AID_{C1},\ AID_{C2},\ \cdots>$$

$$ALIST<AID_A \mid AID_{B1},\ AID_{B2},\ \cdots,\ AID_{C1},\ AID_{C2},\ \cdots> + \text{Enabler of } AID_A + \text{有効期限情報} + \text{移転制御情報}$$

$$\rightarrow PAT<AID_A \mid AID_{B1},\ AID_{B2},\ \cdots,\ AID_{C1},\ AID_{C2},\ \cdots>$$

(3) 分割（Split ＰＡＴ）（図３５参照）：

ＡＬＩＳＴを同一所有者ＡＩＤの複数ＡＬＩＳＴに分解し、分解後のすべてのＡＬＩＳＴに対し、それぞれ、有効期限情報および移転制御情報を設定する。

【数１７】

$$ALIST<AID_A \mid AID_{B1},\ AID_{B2},\ \cdots,\ AID_{C1},\ AID_{C2},\ \cdots> + \text{Enabler}_A$$

$$\rightarrow ALIST<AID_A \mid AID_{B1},\ AID_{B2},\ \cdots> + ALIST<AID_A \mid AID_{C1},\ AID_{C2},\ \cdots>$$

$$ALIST<AID_A \mid AID_{C1},\ AID_{C2},\ \cdots> + \text{Enabler of } AID_A + \text{有効期限情報} + \text{移転制御情報}$$

$$\rightarrow PAT<AID_A \mid AID_{C1},\ AID_{C2},\ \cdots>$$

(4) 所有者変更（Trans ＰＡＴ）（図３６参照）：

ＡＬＩＴＳの所有者ＡＩＤを変更し、変更後のＡＬＩＳＴに対し有効期限情報および移転制御情報を設定する。

【０２３６】

【数１８】

$$ALIST<AID_A \mid AID_B> + ALIST<AID_A \mid AID_{C1},\ AID_{C2},\ \cdots> + \text{Enabler of } AID_A + \text{Enabler of } AID_B$$

$$\rightarrow ALIST<AID_B \mid AID_{C1},\ AID_{C2},\ \cdots>$$

$$ALIST<AID_B \mid AID_{C1},\ AID_{C2},\ \cdots> + \text{Enabler of } AID_B + \text{有効期限情報} + \text{移転制御情報}$$

$$\rightarrow PAT<AID_B \mid AID_{C1},\ AID_{C2},\ \cdots>$$

有効期限情報の設定における操作では、所有者ＡＩＤとこれに対応したEnabler の両者を所有するユーザにのみ有効期限情報の設定を許可するために、以下の操作を定義する。

【０２３７】

【数１９】

$$ALIST<AID_A \mid AID_B>+ \text{Enabler of } A + \text{有効期限情報} \rightarrow PAT<AID_A \mid AID_B>$$

移転制御情報の設定における操作では、所有者ＡＩＤとこれに対応したEnabler の両者を所有するユーザにのみ移転制御情報の設定を許可するために、以下の操作を定義する。

【０２３８】

【数２０】

$$ALIST<AID_A \mid AID_B>+ \text{Enabler of } A + \text{移転制御情報} \rightarrow PAT<AID_A \mid AID_B>$$

次に、本実施形態の全体構成を示す図３７～図４３について説明する。図３７～図４３において、通信網からAID_Aを割り当てられたユーザAは、ユーザAの計算機にAID_Aおよび Enabler of AID_Aを保存し、フロッピードライブ、ＣＤ－ＲＯＭドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、上記仕様と同等の機能を持つ通信端末（電話、携帯電話等）に、AID_Aおよび Enabler of AID_Aを保存している。

【０２３９】

同様に、通信網からAID_Bを割り当てられたユーザBは、自らの計算機にAID_Bおよび Enabler of AID_Bを保存し、フロッピードライブ、ＣＤ－ＲＯＭドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、上記仕様と同等の機能を持つ通信端末（電話、携帯電話等）に、AID_Aおよび Enabler of AID_Aを保存している。

【０２４０】

以下、ユーザAが$PAT<AID_A \mid AID_B>$を生成する手順を説明する。

【０２４１】

(1) ユーザＡは、以下の手段のいずれかを用いて、$ＡＩＤ_B$ および Enabler of $ＡＩＤ_B$ を取得する。

・オンライン検索サービスに$ＡＩＤ_B$ と Enabler of $ＡＩＤ_B$ を登録し、ユーザＡが検索結果として取得するのを待つ（図３７）。

・電子メール、シグナリング等で$ＡＩＤ_B$ と Enabler of $ＡＩＤ_B$ をユーザＡに直接送信する（図３８～図３９）。

・フロッピーディスク、ＣＤ－ＲＯＭ、ＭＯ、ＩＣカード等の磁気、光、電子メディアに$ＡＩＤ_B$ と Enabler of $ＡＩＤ_B$ を蓄積し、ユーザＡに渡す。または、ユーザＡが閲覧して取得するのを待つ（図４０～図４１）。

・書籍、名刺等の紙メディアに$ＡＩＤ_B$ と Enabler of $ＡＩＤ_B$ を記載し、ユーザＡに渡す（図４２～図４３）。もしくは、ユーザＡが閲覧し取得するのを待つ。

【０２４２】

(2) 上述した（１）のいずれかの手段で$ＡＩＤ_B$ および Enabler of $ＡＩＤ_B$ を取得したユーザＡは、ＰＡＴ演算装置に対しMakeＰＡＴ命令を発行する。この手順は図３７～図４３で共通で、以下の通りに定義する。

(a) ユーザＡは、ユーザＡの通信端末に$ＡＩＤ_A$、 Enabler of $ＡＩＤ_A$、$ＡＩＤ_B$、 Enabler of $ＡＩＤ_B$、有効期限情報、および移転制御情報値をセットし、MakeＰＡＴ命令（図５０）の発行を要求する。

(b) ユーザＡの通信端末は、MakeＰＡＴ命令を生成する。

(c) ユーザＡの通信端末は、生成したMakeＰＡＴ命令を電子メール、シグナリング等の手段でＰＡＴ演算装置に送信する（MakeＰＡＴ命令の発行）。

【０２４３】

(d) ＰＡＴ演算装置は、受信したMakeＰＡＴ命令を図４４、図４６、図４７、図５１に従って処理し、$ＰＡＴ＜ＡＩＤ_A$ ｜$ＡＩＤ_B$ ＞を生成する。具体的には、

【数２１】

$$ＡＩＤ_A + ＡＩＤ_B + \text{Enabler of } ＡＩＤ_B + \text{Enabler of } ＡＩＤ_A$$

$$\rightarrow ALIST<AID_A \mid AID_B>$$

$$ALIST<AID_A \mid AID_B> + \text{Enabler of } AID_A$$

＋有効期限情報＋移転制御情報

$$\rightarrow PAT<AID_A \mid AID_B>$$

(e) ＰＡＴ演算装置は、生成した$PAT<AID_A \mid AID_B>$を電子メール、シグナリング等の手段でユーザＡの通信端末、または必要に応じて、ユーザＢの通信端末に送信する。

【０２４４】

(f) ユーザＡ（またはユーザＢ）の通信端末は、受信した$PAT<AID_A \mid AID_B>$をユーザＡの通信端末の記憶装置に保存する。

【０２４５】

ＰＡＴのマージ（Merge ＰＡＴ、図４４、図４６、図４８、図５２）、ＰＡＴの分割（Split ＰＡＴ、図４５、図４６、図４９、図５３）、ＰＡＴの所有者変更（Trans ＰＡＴ、図４４、図４６、図５０、図５４）も同様の手順である。

【０２４６】

次に、MakeＰＡＴ、Merge ＰＡＴ、Trans ＰＡＴの処理の全体の流れを図４４に従って説明する。

【０２４７】

１．新規生成または変更後のＰＡＴの所有者ＡＩＤを決定する（ステップＳ４４１１）。

２．新規生成または変更後のＰＡＴの会員ＡＩＤを決定する（ステップＳ４４１２）。

３．ステップＳ４４１１の所有者ＡＩＤとステップＳ４４１２の会員ＡＩＤを要素に持つＡＩＤリストを生成する（ステップＳ４４１３）。

【０２４８】

４．メッセージから有効期限情報および移転制御情報を抽出する（ステップＳ４４１４）。

【０２４９】

５．ステップＳ４４１３のＡＩＤリストに、ステップＳ４４１４の有効期限情報

および移転制御情報を設定する（ステップＳ４４１５）。

６．ステップＳ４４１５の結果に所有者インデックスを設定する（ステップＳ４４１６）。

７．ステップＳ４４１６の結果にＰＡＴ演算装置の識別子（シリアルナンバー）を設定する（ステップＳ４４１７）。

【０２５０】

８．ステップＳ４４１７の結果にＰＡＴ演算装置の識別子（シリアルナンバー）の秘密鍵で署名する（ステップＳ４４１８）。

【０２５１】

９．ステップＳ４４１８の結果を所有者ＡＩＤ宛に送信し、必要に応じて会員ＡＩＤ宛にも送信する（ステップＳ４４１９）。

【０２５２】

Split ＰＡＴは、MakeＰＡＴ、Merge ＰＡＴ、Trans ＰＡＴとは異なり、複数のＰＡＴを生成する。従って、Split ＰＡＴの処理は図４５に示すように図４４の処理に再帰制御（ステップＳ４４２０）を加えることと定義する。

【０２５３】

次に、所有者ＡＩＤの決定について説明する。新規生成ＰＡＴまたは内容変更後ＰＡＴの所有者ＡＩＤの決定は、以下の手順に従う。

【０２５４】

MakeＰＡＴの場合、所有者ＡＩＤの決定は、図４７に示すように行われる。

【０２５５】

１．図５６のメッセージから、新規生成ＰＡＴの所有者ＡＩＤにしたいＡＩＤを抽出する（ステップＳ４７１１）。

２．上記ＡＩＤが存在する場合には、上記メッセージから、新規生成ＰＡＴの所有者ＡＩＤにしたいＡＩＤのEnabler を抽出する（ステップＳ４７１２，Ｓ４７１３）。

【０２５６】

３．Enabler が存在する場合には、ステップＳ４７１１で抽出したＡＩＤについて、ステップＳ４７１３で抽出したEnabler と対応しているか調べる（ステップ

Ｓ４７１４，Ｓ４７１５）。

４．対応している場合には、抽出したＡＩＤを新規生成ＰＡＴの所有者ＡＩＤに決定し、対応していない場合には、処理を中止する（ステップＳ４７１６，Ｓ４７１７）。

Merge ＰＡＴの場合、所有者ＡＩＤの決定は、図４８に示すように行われる。

【０２５７】

１．図５７のメッセージから、マージ対象のＰＡＴをすべて抽出する（ステップＳ４８１１）。

２．ステップＳ４８１１で抽出したすべてのＰＡＴから、所有者ＡＩＤを抽出する（ステップＳ４８１２）。

３．ステップＳ４８１２で抽出した所有者ＡＩＤを比較し（ステップＳ４８１３）、少なくとも１個の所有者ＡＩＤが一致しない場合、処理を中止し、すべての所有者ＡＩＤが一致する場合、下記処理（ステップＳ４８１４）を実行する。

【０２５８】

４．図５７のメッセージから、マージ後ＰＡＴの所有者ＡＩＤにしたいＡＩＤのEnabler を抽出する（ステップＳ４８１４）。

５．Enabler が存在する場合、ステップＳ４８１３で比較の結果のＡＩＤがステップＳ４８１４で抽出したEnabler と対応しているか調べ（ステップＳ４８１５，Ｓ４８１６）、対応している場合、ステップＳ４８１１で抽出したＡＩＤをマージ後ＰＡＴの所有者ＡＩＤに決定し、対応していない場合、処理を中止する（ステップＳ４８１７，Ｓ４８１８）。

【０２５９】

Split ＰＡＴの場合、所有者ＡＩＤの決定は、図４９に示すように行われる。

【０２６０】

１．図５８のメッセージから、分割対象のＰＡＴを抽出する（ステップＳ４９１１）。

２．ステップＳ４９１１で抽出したＰＡＴから、所有者ＡＩＤを抽出する（ステップＳ４９１２）。

３．図５８のメッセージから、分割後のすべてのＰＡＴの所有者ＡＩＤにしたい

ＡＩＤのEnabler を抽出する（ステップＳ４９１３）。

【０２６１】

４．Enabler が存在する場合、ステップＳ４９１２で抽出したＡＩＤがステップＳ４９１３で抽出したEnabler と対応しているか調べ（ステップＳ４９１４，Ｓ４９１５，Ｓ４９１６）、対応している場合、ステップＳ４９１１で抽出したＡＩＤを分割後のすべてのＰＡＴの所有者ＡＩＤに決定し（ステップＳ４９１７）、対応していない場合、処理を中止する（ステップＳ４９１６）。

【０２６２】

Trans ＰＡＴの場合、所有者ＡＩＤの決定は、図５０に示すように行われる。

【０２６３】

１．図５９のメッセージから、変更対象のＰＡＴを抽出する（ステップＳ５０１１）。

２．この抽出したＰＡＴから、（現在の）所有者ＡＩＤを抽出する（ステップＳ５０１２）。

３．図５９のメッセージから、（現在の）所有者ＡＩＤのEnabler を抽出する（ステップＳ５０１３）。

【０２６４】

４．Enabler が存在する場合、ステップＳ５０１２で抽出したＡＩＤがステップＳ５０１３で抽出したEnabler と対応しているか調べる（ステップＳ５０１４～Ｓ５０１６）。

５．対応している場合、図５９のメッセージから、新しく所有者ＡＩＤにしたいＡＩＤを抽出し、対応していない場合は処理を中止する（ステップＳ５０１７）。

６．上記ＡＩＤが会員ＡＩＤである場合、上記メッセージから、新しく所有者ＡＩＤにしたいＡＩＤのEnabler を抽出する（ステップＳ５０１８，Ｓ５０１９）。

【０２６５】

７．Enabler が存在する場合、ステップＳ５０１７で抽出したＡＩＤがステップＳ５０１９で抽出したEnabler と対応しているか調べ（ステップＳ５０２０～Ｓ

５０２２）、対応している場合ステップＳ５０１７で抽出したＡＩＤを新所有者ＡＩＤに決定し（ステップＳ５０２３）、対応していない場合、処理を中止する（ステップＳ５０２２）。

【０２６６】

次に、会員ＡＩＤの決定について説明する。新規生成ＰＡＴまたは内容変更後ＰＡＴの会員ＡＩＤの決定は、以下の手順に従う。

【０２６７】

MakeＰＡＴの場合、所有者ＡＩＤの決定は、図５１に示すように行われる。

【０２６８】

１．図５６のメッセージから、新規生成ＰＡＴの会員ＡＩＤにしたいＡＩＤをすべて抽出する（ステップＳ５１１１）。

２．ＡＩＤが存在する場合には、図５６のメッセージから、新規生成ＰＡＴの会員ＡＩＤにしたいすべてのＡＩＤについて、それぞれEnabler を抽出する（ステップＳ５１１２，Ｓ５１１３）。

【０２６９】

３．Enabler が存在する場合、ステップＳ５１１１で抽出したすべてのＡＩＤについて、それぞれステップＳ５１１２で抽出したEnabler と対応しているか調べ（ステップＳ５１１４～Ｓ５１１６）、対応しているＡＩＤを新規生成ＰＡＴの会員ＡＩＤに決定し（ステップＳ５１１７）、対応していないＡＩＤを廃棄し、すべての処理対象ＡＩＤについて上記処理を繰り返し行う（ステップＳ５１１８）。

【０２７０】

Merge ＰＡＴの場合、会員ＡＩＤの決定は、図５２に示すように行われる。

【０２７１】

１．図５７のメッセージから、マージ対象のすべてのＰＡＴを抽出する（ステップＳ５２１１）。

２．この抽出したすべてのＰＡＴから、それぞれ（所有者インデックスをもとに）所有者ＡＩＤを抽出する（ステップＳ５２１２）。

３．この抽出したすべての所有者ＡＩＤをマージ後の所有者ＡＩＤに決定したＡ

ＩＤと比較する（ステップＳ５２１３）。

【０２７２】

４．一致する場合には、ＰＡＴから会員ＡＩＤを抽出し（ステップＳ５２１４）、この抽出した会員ＡＩＤをマージ後の会員ＡＩＤに追加する（ステップＳ５２１５）。

【０２７３】

５．一致しない場合、ＰＡＴを削除し、処理対象を次のＰＡＴとして、上記処理を繰り返し行い、処理対象が存在しない場合には、処理を中止する（ステップＳ５２１６）。

【０２７４】

Split ＰＡＴの場合、会員ＡＩＤの決定は、図５３に示すように行われる。

【０２７５】

１．図５８のメッセージから分割対象のＰＡＴを抽出する（ステップＳ５３１１）。

２．この抽出したＰＡＴから所有者ＡＩＤを抽出する（ステップＳ５３１２）。

３．この抽出した所有者ＡＩＤを分割後の所有者ＡＩＤに決定したＡＩＤと比較する（ステップＳ５３１３）。

【０２７６】

４．一致する場合には、メッセージから会員ＡＩＤのリストを抽出し（ステップＳ５３１４）、一致しない場合には、処理を中止する。

５．ステップＳ５３１１のＰＡＴから、ステップＳ５３１４のリストに含まれる会員ＡＩＤをすべて抽出する（ステップＳ５３１５）。

６．この抽出した会員ＡＩＤの組み合わせを分割後の会員ＡＩＤに決定する（ステップＳ５３１６）。

【０２７７】

Trans ＰＡＴの場合、会員ＡＩＤの決定は、図５４に示すように行われる。

【０２７８】

１．図５９のメッセージから所有者変更したいＰＡＴを抽出し、この抽出したＰＡＴからすべての会員ＡＩＤを抽出する（ステップＳ５４１１）。

２．所有者ＡＩＤを変更後ＰＡＴの会員ＡＩＤにするかチェック（ステップＳ５４１２）、会員ＡＩＤにする場合には、ステップＳ５４１１のＰＡＴから所有者ＡＩＤも抽出する（ステップＳ５４１３）。

３．ステップＳ５４１３のＡＩＤを変更後ＰＡＴの会員ＡＩＤに決定する（ステップＳ５４１４）。

【０２７９】

次に、ＡＩＤリストの生成について説明する。ＡＩＤリストの生成は、MakeＰＡＴ、Merge ＰＡＴ、Split ＰＡＴ、Trans ＰＡＴで共通であり、図４６に示すように行われる。

【０２８０】

１．会員ＡＩＤ数をもとに、ＡＩＤリストのバッファ長を決定する（ステップＳ４６１１）。

２．この決定した情報をもとに、バッファを生成する（ステップＳ４６１２）。

３．所有者ＡＩＤをステップＳ４６１２のバッファの空き領域にコピーする（ステップＳ４６１３）。

４．会員ＡＩＤをステップＳ４６１３の残りの空き領域にコピーする（ステップＳ４６１４）。

５．次の会員ＡＩＤが存在する場合には、ステップＳ４６１４に戻り、繰り返し行う（ステップＳ４６１５）。

【０２８１】

次に、Enabler の正当性の検証について説明する。このEnabler の正当性の検証は、MakeＰＡＴ、Merge ＰＡＴ、Split ＰＡＴ、Trans ＰＡＴで共通であり、図５５に示すように行われる。

【０２８２】

１．ＡＩＤとEnabler を入力する（ステップＳ５５１１）。

２．この入力されたＡＩＤとEnabler 中のＡＩＤをＣＡ公開鍵で認証する（ステップＳ５５１２）。改竄されている場合には、処理を中止する（ステップＳ５５１３）。

３．Enabler であることを証明する文字列を入力する（ステップＳ５５１４）。

【０２８３】

４．ステップＳ５５１１のEnabler の先頭フィールドとステップＳ５５１４の文字列を比較する（ステップＳ５５１５）。一致しない場合には、処理を中止する（ステップＳ５５１６）。

５．一致する場合には、ステップＳ５５１１のＡＩＤとEnabler 中のＡＩＤを比較する（ステップＳ５５１７，Ｓ５５１８）。

６．比較処理結果（一致した or 一致しなかった）を出力する（ステップＳ５５１９）。

【０２８４】

次に、上述した実施形態を一元管理型メーリングリストに適用した例について図６０を参照して説明する。コンピュータネットワーク上のグループ通信にメーリングリストがある。以下、メーリングリストにおける連絡先情報管理への適用例を説明する。

【０２８５】

一般に、メーリングリストにおける連絡先リスト（会員のメールアドレスから構成されるリストであり、以後、会員リストと呼ぶ）は、主催者がアクセス可能なインターネット上のサーバ（または、パソコン通信のホスト）において一元的に管理されている（インターネット上のサーバとしては、listserverが広く利用されている）。

【０２８６】

サーバ（ホスト）の主な仕事は：

(1) メーリングリストへの入会申請者から入会届を受信したら、入会申請者のメールアドレスを会員リストに追加する、

(2) メーリングリストからの退会申請者から退会届を受信したら、退会申請者のメールアドレスを会員リストから削除する、

の２点である。

【０２８７】

入会届、退会届の書式は、一般に、入会希望、退会希望を定型化した命令、もしくはこれらを意味する自然言語（例えば「入会したい」という意味を持つ日本

語文字列）と、入会申請者、退会申請者のメールアドレスから構成される。例えば、listserverの場合には、

(1) 入会届

subscribe メーリングリスト名　自分のメールアドレス

(2) 退会届

unsubscribe メーリングリスト名　自分のメールアドレス

とインターネットメールの本文に記述する。

【０２８８】

まず、入会処理について説明する。図６０において、オンライン検索サービスは、ＡＤＳ同様、検索時に検索者ＡＩＤと検索者ＡＩＤのEnabler を送信すると、検索者に対しＰＡＴ＜検索者ＡＩＤ｜登録者ＡＩＤ＞を通知する。以下、入会処理の流れを説明する。

【０２８９】

１．主催者ＡＩＤ登録：主催者は、主催者ＡＩＤ、 Enabler of 主催者ＡＩＤ、申請用の有効期限情報、申請用の移転制御情報、および公開情報をオンライン検索サービスに登録する。

【０２９０】

２．入会申請用ＰＡＴ発行：申請者が検索条件、申請者ＡＩＤ、および Enabler of 申請者ＡＩＤを送信すると、オンライン検索サービスは以下の手順に従いＰＡＴ＜申請者ＡＩＤ｜主催者ＡＩＤ＞を発行する。

【０２９１】

(1) オンライン検索サービスは以下のMakeＰＡＴ命令を生成し、ＰＡＴ演算装置に送信する。

MakeＰＡＴ

申請者ＡＩＤ Enabler of 申請者ＡＩＤ

主催者ＡＩＤ Enabler of 主催者ＡＩＤ

申請用の有効期限情報

申請用の移転制御情報

(2) ＰＡＴ演算装置は、受信したMakeＰＡＴ命令を解釈し、ＰＡＴ＜主催者Ａ

ＩＤ｜申請者ＡＩＤ＞を生成する。具体的には、

【数２２】

申請者ＡＩＤ＋主催者ＡＩＤ＋ Enabler of 主催者ＡＩＤ

＋ Enabler of 申請者ＡＩＤ

→ＡＬＩＳＴ＜主催者ＡＩＤ｜申請者ＡＩＤ＞

ＡＬＩＳＴ＜申請者ＡＩＤ｜主催者ＡＩＤ＞

＋ Enabler of 申請者ＡＩＤ＋申請用の有効期限情報

＋申請用の移転制御情報

→ＰＡＴ＜申請者ＡＩＤ｜主催者ＡＩＤ＞

(3) ＰＡＴ演算装置は、生成したＰＡＴ＜申請者ＡＩＤ｜主催者ＡＩＤ＞をオンライン検索サービスに送信する。

【０２９２】

(4) ＰＡＴ＜申請者ＡＩＤ｜主催者ＡＩＤ＞を受信したオンライン検索サービスは、このＰＡＴを検索結果として申請者に送信する。

【０２９３】

３．入会申請：入会申請者は、入会申請の旨とＰＡＴ＜申請者ＡＩＤ｜主催者ＡＩＤ＞、申請者ＡＩＤ、 Enabler of 申請者を主催者に送信する。

【０２９４】

４．会員登録：申請者ＡＩＤを会員リストＰＡＴ＜主催者ＡＩＤ｜既会員ＡＩＤ＞に登録するまでの流れを以下に説明する。

【０２９５】

(1) 主催者は、以下のTrans ＰＡＴ命令を生成してＰＡＴ演算装置に送信する。

【０２９６】

Trans ＰＡＴ

ＰＡＴ＜申請者ＡＩＤ｜主催者ＡＩＤ＞

申請者ＡＩＤ Enabler of 申請者ＡＩＤ

主催者ＡＩＤ Enabler of 主催者ＡＩＤ

任意の（テンポラリな）有効期限情報

任意の（テンポラリな）移転制御情報

(2) 上記Trans ＰＡＴ命令を受信したＰＡＴ演算装置は、ＰＡＴ＜主催者ＡＩＤ｜申請者ＡＩＤ＞を生成し、このＰＡＴを主催者に送信する。具体的には、

【数２３】

ＡＬＩＳＴ＜申請者ＡＩＤ｜主催者ＡＩＤ＞

＋ Enabler of 申請者ＡＩＤ＋ Enabler of 主催者ＡＩＤ

→ＡＬＩＳＴ＜主催者ＡＩＤ｜申請者ＡＩＤ＞

ＡＬＩＳＴ＜主催者ＡＩＤ｜申請者ＡＩＤ＞＋ Enabler of 主催者ＡＩＤ

＋任意の有効期限情報＋任意の移転制御情報

→ＰＡＴ＜主催者ＡＩＤ｜申請者ＡＩＤ＞

(3) ＰＡＴ演算装置は、生成したＰＡＴ＜主催者ＡＩＤ｜申請者ＡＩＤ＞を主催者に送信する。

【０２９７】

(4) 主催者は、ＰＡＴ＜主催者ＡＩＤ｜申請者ＡＩＤ＞を受信したら、以下のMerge ＰＡＴ命令を生成してＰＡＴ演算装置に送信する。

【０２９８】

Merge ＰＡＴ

ＰＡＴ＜主催者ＡＩＤ｜既会員ＡＩＤ＞

ＰＡＴ＜主催者ＡＩＤ｜申請者ＡＩＤ＞

Enabler of 主催者ＡＩＤ

正式な有効期限情報

正式な移転制御情報

(5) 上記Merge ＰＡＴ命令を受信したＰＡＴ演算装置は、ＰＡＴ＜主催者ＡＩＤ｜既会員ＡＩＤ、申請者ＡＩＤ＞を生成する。具体的には、

【数２４】

ＡＬＩＳＴ＜主催者ＡＩＤ｜既会員ＡＩＤ＞

＋ＡＬＩＳＴ＜主催者ＡＩＤ＋申請者ＡＩＤ＞

＋ Enabler of 主催者ＡＩＤ

→ＡＬＩＳＴ＜主催者ＡＩＤ｜既会員ＡＩＤ、申請者ＡＩＤ＞

ＡＬＩＳＴ＜主催者ＡＩＤ｜既会員ＡＩＤ、申請者ＡＩＤ＞

＋ Enabler of 主催者ＡＩＤ＋会員リストの正式な有効期限情報

＋会員リストの正式な移転制御情報

→ＰＡＴ＜主催者ＡＩＤ｜既会員ＡＩＤ、申請者ＡＩＤ＞

(6) ＰＡＴ演算装置は、生成したＰＡＴ＜主催者ＡＩＤ｜既会員ＡＩＤ、申請者ＡＩＤ＞を主催者に送信する。

【０２９９】

５．通知：主催者は、ＰＡＴ＜主催者ＡＩＤ｜既会員ＡＩＤ、申請者ＡＩＤ＞を申請者に電子メールで送信する。

【０３００】

退会処理は、上記した３．入会申請～５．通知と同様の流れで行われる。

【０３０１】

なお、オンライン検索サービス以外で主催者ＡＩＤが提供された場合、すなわちフロッピーディスク、ＣＤ－ＲＯＭ、紙メディア等で主催者ＡＩＤが提供された場合には、入会申請者は、図３８～図４３のいずれかの手順でＰＡＴ＜申請者ＡＩＤ｜主催者ＡＩＤ＞を生成する。以後は、上述した３．入会申請～５．通知と同様の流れで行う。

【０３０２】

次に、図６１～図６４を参照して、本発明の第３の実施形態について説明する。

【０３０３】

上述した実施形態における個別化アクセスチケット（ＰＡＴ）の新規生成（MakePAT）およびマージ（Merge ＰＡＴ）では、会員ＡＩＤと Enabler of 会員ＡＩＤを個別化アクセスチケットの所有者に渡すことが必要であるが、これを所有者に渡すと、その所有者が別の所有者の主催するグループ通信に対して、取得した会員ＡＩＤで参加することが可能になる。すなわち、会員ＡＩＤを用いた成りすましが可能になるという問題がある。また、その所有者が取得した会員ＡＩＤおよび Enabler of 会員ＡＩＤを不特定多数が閲覧可能なメディアに掲載すれば、誰でもその会員ＡＩＤにアクセス可能になるため、会員ＡＩＤのユーザへの

嫌がらせが発生する恐れがあるとともに、また第三者による会員ＡＩＤを用いた成りすましも可能になるという問題がある。

【０３０４】

そこで、本実施形態では、 Enabler of 会員ＡＩＤを所有者ＡＩＤに渡さなくても、MakeＰＡＴおよびMerge ＰＡＴを可能にする。

【０３０５】

このために、本実施形態では、Ｎｕｌｌ－ＡＩＤ（AID_{Null}）および該Ｎｕｌｌ－ＡＩＤの Enabler(Enabler of Ｎｕｌｌ－ＡＩＤまたは Enabler of AID_{Null}）を使用して、個別化アクセスチケット（ＰＡＴ）の新規生成および既存の個別化アクセスチケット（ＰＡＴ）の内容変更を行うものである。ここで、Ｎｕｌｌ－ＡＩＤを含む演算は、以下のすべての規則に従う：

(a) 上述した実施形態における新規生成（MakeＰＡＴ）、マージ（Merge ＰＡＴ）、分割（Split ＰＡＴ）、変更（Trans ＰＡＴ）からなる演算規則、

(b) Ｎｕｌｌ－ＡＩＤにのみ適用可能な規則として、

i．Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知であり、

ii． Enabler of Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知である。

【０３０６】

ここで、上述した実施形態で定義した演算規則について説明する。

【０３０７】

(1) 複数ＡＩＤからＰＡＴを作る（MakeＰＡＴ）：

【数２５】

$$AID_{所有者} + AID_{会員1} + AID_{会員2} +, \cdots, + AID_{会員N} + \text{Enabler of } AID_{会員1} + \text{Enabler of } AID_{会員2} +, \cdots, + \text{Enabler of } AID_{会員N} + \text{Enabler of } AID_{所有者} \rightarrow PAT<AID_{所有者} \mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$$

(2) 同一所有者の複数ＰＡＴをマージする（Merge ＰＡＴ）：

【数２６】

$$PAT<AID_{所有者} \mid AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}> + PAT<AID_{所有者} \mid AID_{会員b1}, AID_{会員b2}, \cdots,$$

$AID_{会員bN}>$

＋ Enabler of $AID_{所有者}$

→$PAT<AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}, AID_{会員b1}, AID_{会員b2}, \cdots, AID_{会員bN}>$

(3) ＰＡＴを同一所有者の複数ＰＡＴに分割する（Split ＰＡＴ）：

【数２７】

$PAT<AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}, AID_{会員b1}, AID_{会員b2}, \cdots, AID_{会員bN}>$

＋ Enabler of $AID_{所有者}$

→$PAT<AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}>$

＋$PAT<AID_{所有者} | AID_{会員b1}, AID_{会員b2}, \cdots, AID_{会員bN}>$

(4) ＰＡＴの所有者ＡＩＤを変更する（Trans ＰＡＴ）：

【数２８】

$PAT<AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}>$

＋$PAT<AID_{所有者} | AID_{新所有者}>$

＋ Enabler of $AID_{所有者}$＋ Enabler of $AID_{新所有者}$

→$PAT<AID_{新所有者} | AID_{会員a1}, AID_{会員a2}, \cdots, AID_{会員aM}>$

次に、Ｎｕｌｌ－ＡＩＤに関する演算例について説明する：

(1) AID_A と Enabler of AID_A とから$PAT<AID_{Null} | AID_A>$ を作る場合：

(a) Ｎｕｌｌ－ＡＩＤの規則１(b)i. および１(b)ii.より、AID_{Null}と Enabler of AID_{Null}は既知である。

【０３０８】

(b) MakeＰＡＴにより

【数２９】

$AID_{Null}+AID_A$ ＋ Enabler of AID_A ＋ Enabler of AID_{Null}

→ＰＡＴ＜AID_{Null}｜AID_A＞

(2) ＰＡＴ＜AID_{Null}｜AID_A＞とＰＡＴ＜AID_{Null}｜AID_B＞とからＰＡＴ＜AID_{Null}｜AID_A，AID_B＞を作る場合：

(a) Ｎｕｌｌ－ＡＩＤの規則１(b)i．および１(b)ii.より、AID_{Null}とEnabler of AID_{Null}は既知である。

【０３０９】

(b) Merge ＰＡＴにより

【数３０】

ＰＡＴ＜AID_{Null}｜AID_A＞＋ＰＡＴ＜AID_{Null}｜AID_B＞
＋ Enabler of AID_{Null}
→ＰＡＴ＜AID_{Null}｜AID_A，AID_B＞

(3) ＰＡＴ＜AID_{Null}｜AID_A＞とＰＡＴ＜AID_{Null}｜AID_B＞とEnabler of AID_A とからＰＡＴ＜AID_A ｜AID_B＞を作る場合：

(a) Ｎｕｌｌ－ＡＩＤの規則１(b)i．および１(b)ii.より、AID_{Null}とEnabler of AID_{Null}は既知である。

【０３１０】

(b) Trans ＰＡＴにより

【数３１】

ＰＡＴ＜AID_{Null}｜AID_A＞＋ＰＡＴ＜AID_{Null}｜AID_B＞
＋ Enabler of AID_{Null}＋ Enabler of AID_A
→ＰＡＴ＜AID_A ｜AID_B＞

Ｎｕｌｌ－ＡＩＤのデータ構造は、図６１に示すように、Ｎｕｌｌ－ＡＩＤであることを一意に表す文字列（例えば、この文字列の値は認証局ＣＡで定義される）および該文字列に対して認証局ＣＡの署名を施したもので構成される。

【０３１１】

また、Enabler of Ｎｕｌｌ－ＡＩＤのデータ構造は、図６２に示すように、Enabler であることを一意に表す文字列（例えば、この文字列は認証局ＣＡで定義される）、Ｎｕｌｌ－ＡＩＤの実体、および前記Enabler であることを表す文字列と前記Ｎｕｌｌ－ＡＩＤの実体を連結した文字列に対して認証局ＣＡの署名

を施したもので構成される。

【０３１２】

なお、Ｎｕｌｌ－ＡＩＤおよびEnabler of Ｎｕｌｌ－ＡＩＤは、セキュアなＰＡＴ演算装置およびセキュアなＰＡＴ認証局で保持される。

【０３１３】

次に、本実施形態の第１の応用例について図６３を参照して説明する。図６３において、

(1) ユーザＢ（ＰＡＴ会員）は、ユーザＢの端末と接続されたセキュアなＰＡＴ演算装置で前記Ｎｕｌｌ－ＡＩＤに関する演算例（１）を実行してＰＡＴ＜AID_{Null}｜AID_B＞を生成し、任意の手段でユーザＡ（ＰＡＴ所有者）に渡す。

【０３１４】

(2) ＰＡＴ＜AID_{Null}｜AID_B＞を受信したユーザＡは、ユーザＡの端末に接続されたセキュアなＰＡＴ演算装置で

(a) Ｎｕｌｌ－ＡＩＤに関する演算例（１）を実行してＰＡＴ＜AID_{Null}｜AID_A＞を作る。

【０３１５】

(b) Ｎｕｌｌ－ＡＩＤに関する演算例（３）を実行してＰＡＴ＜AID_A｜AID_B＞を作る。

【０３１６】

(3) ユーザＡは、生成したＰＡＴ＜AID_A｜AID_B＞を任意の手段でユーザＡに渡す。

【０３１７】

なお、有効期限の決定方法は前述した方法と共通のため省略する。また、Ｎｕｌｌ－ＡＩＤに関する演算の処理は前述した方法と共通のため省略する。

【０３１８】

ＰＡＴ＜AID_{Null}｜AID_A，AID_B＞をユーザＢに渡す場合には、上述した演算（２）において、前記Ｎｕｌｌ－ＡＩＤに関する演算例（２）を実行する。

【０３１９】

次に、本実施形態の第２の応用例について図６４を参照して説明する。図６４において、

(1) ユーザＢ（ＰＡＴ会員）は、ユーザＢの端末と接続されたセキュアなＰＡＴ演算装置でＮｕｌｌ－ＡＩＤに関する演算例（１）を実行してＰＡＴ＜AID_{Null}｜AID_B＞を作り、任意の公開情報とともにオンライン検索サービス（データベース）に登録する。

【０３２０】

(2) ユーザＡ（ＰＡＴ所有者）は、ユーザＡの端末に接続されたセキュアなＰＡＴ演算装置でユーザＢの端末と接続されたセキュアなＰＡＴ演算装置でＮｕｌｌ－ＡＩＤに関する演算例（１）を実行してＰＡＴ＜AID_{Null}｜AID_A＞を作り、任意の検索条件とともにオンライン検索サービスに提示する。

【０３２１】

(3) ユーザＢの個人情報がユーザＡの提示した検索条件を満足した場合、オンライン検索サービスに接続されたセキュアなＰＡＴ演算装置は

(a) Ｎｕｌｌ－ＡＩＤに関する演算例（２）を実行してＰＡＴ＜AID_{Null}｜AID_A，AID_B＞を作る。

【０３２２】

(b) ＰＡＴ＜AID_{Null}｜AID_A，AID_B＞をオンライン検索サービスに渡す。

【０３２３】

(1) オンライン検索サービスは、ＰＡＴ演算装置で作られたＰＡＴ＜AID_{Null}｜AID_A，AID_B＞をユーザＡに渡す。

【０３２４】

(2) ＰＡＴ＜AID_{Null}｜AID_A，AID_B＞を受け取ったユーザＡは、ユーザＡの端末に接続されたセキュアなＰＡＴ演算装置で下記のTrans ＰＡＴ演算を実行して、ＰＡＴ＜AID_A｜AID_B＞を作る。

【０３２５】

【数３２】

$$PAT<AID_{Null}\mid AID_A>$$
$$+PAT<AID_{Null}\mid AID_A, AID_B>$$
$$+\ \text{Enabler of}\ AID_{Null}+\ \text{Enabler of}\ AID_A$$
$$\rightarrow PAT<AID_A\mid AID_B>$$

尚、有効期限の決定方法は前述した方法と共通のため省略する。また、Ｎｕｌｌ－ＡＩＤに関する演算の処理は前述した方法と共通のため省略する。

【０３２６】

$PAT<AID_A\mid AID_B>$をオンライン検索サービスに接続されたセキュアなＰＡＴ演算装置で生成する場合には、そのＰＡＴ演算装置に Enabler of AID_A を渡す。そして、上述した演算（３）において、Ｎｕｌｌ－ＡＩＤに関する演算例（３）を実行する。

【０３２７】

$PAT<AID_B\mid AID_A>$をオンライン検索サービスに接続されたセキュアなＰＡＴ演算装置で生成して、ユーザＢに渡す場合には、そのＰＡＴ演算装置に Enabler of AID_B を渡す。そして、上述した演算（３）において、Ｎｕｌｌ－ＡＩＤに関する演算例（３）と同様の演算を実行する。

【０３２８】

次に、本発明の第４の実施形態について図６５～図６８を参照して説明する。

【０３２９】

グループ通信においては参加者を固定したい状況はしばしば発生するが、上述した実施形態では個別化アクセスチケット（ＰＡＴ）を変更不可にする機能を持たないため、参加者を固定することができない。すなわち、上述した実施形態では、参加者を固定するか否かは、個別化アクセスチケットの所有者の判断に一任されている。

【０３３０】

そこで、本実施形態では、個別化アクセスチケットに読取専用属性を設定している。

【０３３１】

このため、本実施形態では、Ｇｏｄ－ＡＩＤ（AID_{God}）を用いて、個別化アクセスチケット（ＰＡＴ）に読取専用属性を設定している。ここで、Ｇｏｄ－ＡＩＤに関する演算は、以下のすべての規則に従う：

(a) Ｇｏｄ－ＡＩＤは、すべてのユーザに既知であり、

(b) Ｇｏｄ－ＡＩＤに関する演算は、以下のいずれかのみ許可される：

【数３３】

i．$AID_{所有者}$がAID_{Null}でもAID_{God}でもない場合：

$$PAT<AID_{所有者}\mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}> + \text{Enabler of } AID_{所有者} \rightarrow PAT<AID_{God}\mid AID_{所有者}, AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$$

ii．$AID_{所有者}$がAID_{Null}の場合：

$$PAT<AID_{Null}\mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}> + \text{Enabler of } AID_{Null} \rightarrow PAT<AID_{God}\mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$$

Ｇｏｄ－ＡＩＤのデータ構造は、図６５に示すように、Ｇｏｄ－ＡＩＤであることを一意に表す文字列（例えば、この文字列の値は認証局ＣＡで定義される）および該文字列に対して認証局ＣＡの署名を施したものから構成される。Ｇｏｄ－ＡＩＤは、上述したセキュアなＰＡＴ演算装置およびセキュアなＰＡＴ認証局で保持されている。

【０３３２】

Ｇｏｄ－ＡＩＤ規則の処理について図６６に示すフローチャートを参照して説明する。図６６において、

１．個別化アクセスチケットの所有者ＡＩＤと、Ｎｕｌｌ－ＡＩＤとＧｏｄ－ＡＩＤを入力する（ステップＳ６６１１）。

【０３３３】

２．ステップＳ６６１１で入力した所有者ＡＩＤとＧｏｄ－ＡＩＤを文字列比較する（ステップＳ６６１３）。

【０３３４】

・完全に一致するか否かをチェック（ステップＳ６６１５）、完全に一致する場合には、処理を中止するが、一部でも一致しなかった場合には、次のステップＳ６６１７に進む。

【０３３５】

３．上記所有者ＡＩＤをステップＳ６６１１で入力したＮｕｌｌ－ＡＩＤと文字列比較する（ステップＳ６６１７）。

【０３３６】

(a) 完全に一致するか否かをチェックし（ステップＳ６６１９）、完全に一致する場合には、

ｉ．Enabler of Ｎｕｌｌ－ＡＩＤを入力する（ステップＳ６６２１）。

【０３３７】

ii．上記所有者ＡＩＤ（すなわち、Ｎｕｌｌ－ＡＩＤ）とステップＳ６６２１で入力した Enabler of Ｎｕｌｌ－ＡＩＤを用いて、 Enabler of Ｎｕｌｌ－ＡＩＤの正当性を判定する（ステップＳ６６２３）（尚、判定手順は図５５に従う）。

【０３３８】

・ Enabler of Ｎｕｌｌ－ＡＩＤがＮｕｌｌ－ＡＩＤの正当なEnabler である場合（ステップＳ６６２３）、所有者ＡＩＤ（すなわち、Ｎｕｌｌ－ＡＩＤ）をＧｏｄ－ＡＩＤで上書きしてから、終了する（ステップＳ６６２５）。

【０３３９】

・ Enabler of Ｎｕｌｌ－ＡＩＤがＮｕｌｌ－ＡＩＤの正当なEnabler でない場合には、処理を中止する。

【０３４０】

(b) ステップＳ６６１９の判定において、一部でも一致しない場合、

ｉ．Enabler of 所有者ＡＩＤを入力する（ステップＳ６６２７）。

【０３４１】

ii. 上記所有者ＡＩＤとステップＳ６６２７で入力した Enabler of 所有者ＡＩＤを用いて、 Enabler of 所有者ＡＩＤの正当性を判定する（判定手順は図５５に従う）（ステップＳ６６２９）。

【０３４２】

・ Enabler of 所有者ＡＩＤが所有者ＡＩＤの正当なEnabler である場合（ステップＳ６６３１）、ステップＳ６６３３へ進む。

【０３４３】

・ Enabler of 所有者ＡＩＤが所有者ＡＩＤの正当なEnabler でない場合（ステップＳ６６３１）、処理を中止する。

【０３４４】

iii. Ｇｏｄ－ＡＩＤを個別化アクセスチケットＰＡＴに連結する（ステップＳ６６３３）。

【０３４５】

iv. 個別化アクセスチケットＰＡＴの所有者Index をＧｏｄ－ＡＩＤに設定する（ステップＳ６６３５）。

【０３４６】

次に、本実施形態の応用例について図６７を参照して説明する。

【０３４７】

$PAT<AID_{Null}|AID_A>$と$PAT<AID_{Null}|AID_B>$とから$PAT<AID_{God}|AID_A, AID_B>$を作る場合、ＰＡＴ所有者（図６７におけるユーザA）の端末に接続されたセキュアなＰＡＴ演算装置において、以下の演算を実行する。

【０３４８】

(1) 上述した新規生成の演算規則Merge ＰＡＴにより

【数３４】

$$PAT<AID_{Null}|AID_A>+PAT<AID_{Null}|AID_B>$$
$$+\ \text{Enabler of}\ AID_{Null}$$
$$\rightarrow PAT<AID_{Null}|AID_A, AID_B>$$

(2) Ｇｏｄ－ＡＩＤに関する演算規則（ａ）より、AID_{God} は既知である。

【０３４９】

(3) Ｇｏｄ－ＡＩＤに関する演算規則(b)ii.より

【数３５】

$$PAT<AID_{Null}\mid AID_A, AID_B>$$
$$+ \text{Enabler of } AID_{Null}$$
$$\rightarrow PAT<AID_{God}\mid AID_A, AID_B>$$

上記演算は、第三者の計算機（サーチエンジンなど）に接続されたセキュアなＰＡＴ演算装置（図６８）またはセキュアな認証局でも実行される。

【０３５０】

次に、図６９を参照して、本発明の第５の実施形態について説明する。

【０３５１】

上述した第３の実施形態で説明したように、Ｎｕｌｌ－ＡＩＤを追加すると、以下に説明するように、個別化アクセスチケット（ＰＡＴ）の所有者（所有者ＡＩＤのユーザ）が会員（会員ＡＩＤのユーザ）へのアクセス権を第三者に委譲できるようになるという問題がある。しかも、会員に無断で委譲可能である。

【０３５２】

１．$PAT<AID_A\mid AID_B>$の所有者Ａが（会員はＢ）

・$PAT<AID_A\mid AID_B>$

・AID_A

・ Enabler of AID_A

を用いて、$PAT<AID_{Null}\mid AID_B>$を作る。ここで、Ａは、$PAT<AID_A\mid AID_B>$に加えて

・AID_A

・ Enabler of AID_A

・AID_{Null}

・ Enabler of AID_{Null}

をすべて知っているとする。

【０３５３】

(a) Aは、MakePATにより、PAT<AID_A | AID_{Null}>を作る。

【０３５４】

【数３６】

AID_A +AID_{Null}+ Enabler of AID_{Null}+ Enabler of AID_A

→PAT<AID_A | AID_{Null}>

(b) Aは、Trans PATにより、PAT<AID_{Null} | AID_B >を作る。

【０３５５】

【数３７】

PAT<AID_A | AID_B >+PAT<AID_A | AID_{Null}>

+ Enabler of AID_A + Enabler of AID_{Null}

→PAT<AID_{Null} | AID_B >

上記１(b) の後、AがPAT<AID_{Null} | $AID_{会員}$>を第三者Cに渡すと

【０３５６】

２．Cは、PAT<AID_{Null} | AID_B >を用いて、PAT<AID_C | AID_B >を作る。ここで、Cは、PAT<AID_{Null} | $AID_{会員}$>に加えて

・AID_C

・ Enabler of AID_C

・AID_{Null}

・ Enabler of AID_{Null}

をすべて知っているとする。

【０３５７】

(a) Cは、MakePATにより、PAT<AID_{Null} | AID_C >を作る。

【０３５８】

【数３８】

AID_{Null}+AID_C + Enabler of AID_{Null}+ Enabler of AID_C

→PAT<AID_{Null} | AID_C >

(b) Cは、Trans PATにより、PAT<AID_C | AID_B >を作る。

【０３５９】

【数３９】

$$PAT<AID_{Null}\mid AID_B>+PAT<AID_{Null}\mid AID_C>$$
$$+\ \text{Enabler of}\ AID_{Null}+\ \text{Enabler of}\ AID_C$$
$$\rightarrow PAT<AID_C\mid AID_B>$$

上記２(b) の結果、ＣはＰＡＴ＜AID_C ｜AID_B ＞を得るので、Ｂへのアクセスが可能になる。

【０３６０】

そこで、本実施形態では、ＰＡＴ＜$AID_{所有者}$｜$AID_{会員}$＞の所有者が$AID_{会員}$のEnabler を知らない場合には、このＰＡＴからＰＡＴ＜AID_{Null}｜$AID_{会員}$＞を作ることができないようにする。

【０３６１】

このため、本実施形態では、ＰＡＴの所有者が$AID_{会員}$のEnabler なしでＰＡＴ＜AID_{Null}｜$AID_{会員}$＞を作るためには、ＰＡＴ＜$AID_{所有者}$｜AID_{Null}＞を作ることが必要になる。

【０３６２】

そこで、上述した第３の実施形態で説明したＮｕｌｌ－ＡＩＤに対して、以下の規則を追加する。

【０３６３】

Ｎｕｌｌ－ＡＩＤはＰＡＴの所有者ＡＩＤとしてのみ使用できる（会員ＡＩＤとしては使用できない）。

【０３６４】

・ＰＡＴ＜AID_{Null}｜$AID_{会員1}$，$AID_{会員2}$，…，$AID_{会員N}$＞は許可する。

【０３６５】

・ＰＡＴ＜$AID_{所有者}$｜AID_{Null}，$AID_{会員1}$，$AID_{会員2}$，…，$AID_{会員N}$＞は許可しない。

【０３６６】

上述した実施形態におけるセキュアなＰＡＴ演算装置とセキュアなＰＡＴ認証

局にそれぞれＮｕｌｌ－ＡＩＤが会員ＡＩＤに含まれているか否かをチェックする機能を追加する。この会員ＡＩＤのチェック処理機能について図６９に示すフローチャートを参照して説明する。図６９において、

１．Ｎｕｌｌ－ＡＩＤとＰＡＴを入力する（ステップＳ６９１１）。

【０３６７】

２．ステップＳ６９１１で入力したＰＡＴから、会員ＡＩＤをすべて抽出する（ステップＳ６９１３）。

【０３６８】

３．この抽出したすべての会員ＡＩＤについて、それぞれ、ステップＳ６９１１で入力したＮｕｌｌ－ＡＩＤと文字列比較する（ステップＳ６９１５）。

【０３６９】

・すべての会員ＡＩＤがＮｕｌｌ－ＡＩＤと完全に一致しない場合（ステップＳ６９１７，Ｓ６９１９）、Merge ＰＡＴ、Split ＰＡＴ、またはTrans ＰＡＴ処理に移る（図４４または図４５）（ステップＳ６９２１）。

【０３７０】

・会員ＡＩＤが１つでもＮｕｌｌ－ＡＩＤと完全に一致する場合（ステップＳ６９１７）、処理を中止する。

【０３７１】

次に、図７０～図８０を参照して、本発明の第６の実施形態について説明する。この第６の実施形態は、上述した第１の実施形態において図３に示した役割識別子ＡＩＤに対して後述する図７１（ｂ）のようにリンク情報を追加するとともに、図３に示した１対１個別化アクセスチケットＰＡＴに含まれていた役割識別子ＡＩＤの実体の代わりに前記役割識別子ＡＩＤのリンク情報を図７１（ｃ）に示すように設定し、該リンク情報で役割識別子ＡＩＤを一意に特定するように構成した点が異なるものである。

【０３７２】

なお、このようにリンク情報を追加された役割識別子ＡＩＤをリンク情報付き役割識別子ＡＩＤと称し、ＡＩＤのリンク情報を有する１対１個別化アクセスチケットＰＡＴをリンク指定型１対１個別化アクセスチケットＰＡＴと称すること

にする。また、リンク情報は、役割識別子ＡＩＤを一意に特定可能な情報であり、認証局ＣＡによって役割識別子ＡＩＤに対して一意に付与されるシリアル番号である。

【０３７３】

まず、図７０を参照して、本発明の第６の実施形態の全体構成図について説明する。図７０において、１は認証局ＣＡであり、認証権限と役割識別子ＡＩＤの発行権限を有し、ユーザに対して役割識別子を割り当てる機能を有する。３はユーザあり、５はセキュア・コミュニケーション・サービスＳＣＳであり、ユーザ３間の電子メールを転送し、必要に応じて着信拒否および個人識別子の同一性を判定し、取り出す。７はアノニマス・ディレクトリ・サービスＡＤＳであり、役割識別子ＡＩＤ、移転制御情報、有効期限、および、プライバシー情報を管理するデータベースである。すなわち、アノニマス・ディレクトリ・サービスＡＤＳ７は、検索者の役割識別子ＡＩＤと検索条件（一般に、プライバシー情報）にマッチした登録者の役割識別子ＡＩＤから個別化アクセスチケットＰＡＴを発行し、検索者に交付する機能を有する。

【０３７４】

ユーザの要求に基づいて個人識別子から役割識別子ＡＩＤを生成し、そのユーザに割り当てるまでの一連の処理はリンク情報が付加されることを除いて第１の実施形態と基本的に同じであるが、具体的に図７１を参照して説明する。

【０３７５】

図７１は、個人識別子ＯＩＤ(Official Identification) とリンク情報付き役割識別子ＡＩＤの例を示している。同図に示すように、個人識別子ＯＩＤは、図７１（ａ）に示すように認証局ＣＡ１がユーザに一意に生成した任意の文字列に対して認証局ＣＡ１が秘密鍵で電子署名したものである。また、リンク情報付き役割識別子ＡＩＤは、図７１（ｂ）に示すように個人識別子ＯＩＤの一部とその位置情報、冗長な文字列、ＳＣＳのホストＯＩＤ、およびリンク情報からなる文字列に対し、認証局ＣＡ１の秘密鍵で電子署名を施したものである。

【０３７６】

また、リンク指定型１対１個別化アクセスチケットＰＡＴは、図７１（ｃ）に

示すように、発信者フラグ、移転制御フラグ、役割識別子$ＡＩＤ_0$のリンク情報、役割識別子$ＡＩＤ_1$のリンク情報、有効期限からなる文字列に対してアノニマス・ディレクトリ・サービスＡＤＳのＯＩＤ秘密鍵による電子署名を施したものである。

【０３７７】

ユーザ３がリンク情報付き役割識別子ＡＩＤを認証局ＣＡ１に対して請求する処理は、図４に示したフローチャートを参照した上述した説明と同じである。

【０３７８】

次に、上述した役割識別子ＡＩＤの請求に対する認証局ＣＡ１が役割識別子ＡＩＤをユーザ３に対して交付する処理も図５に示すフローチャートを参照した説明と同じである。

【０３７９】

ユーザにおけるＡＩＤ交付処理も図６を参照した説明と同じである。

【０３８０】

次に、認証局ＣＡにおける役割識別子ＡＩＤの生成処理について図７２、図７３を参照して説明する。図７２において、認証局ＣＡ１は乱数発生等の任意の手段を用いて、個人識別子ＯＩＤの全長Ｌと等しい長さの文字列を生成し、この文字列を仮の役割識別子ＡＩＤとして生成する（ステップＳ９１１）。

【０３８１】

次に、個人識別子ＯＩＤの複写を行うために、個人識別子ＯＩＤのコピー範囲を指定するｐとｌの値を決定する（ステップＳ９１３）。これは、乱数発生等の任意の手段を用いて、パラメータp_iとl_iの値をそれぞれ$0 \leqq p_i \leqq L$および$l_{min} \leqq l_i \leqq l_{Max}$のようにコピー範囲を決定する。ここで、Ｌは個人識別子ＯＩＤの全長であり、l_{min}およびl_{Max}は$0 < l_{min} < l_{Max} < L$が成り立つ範囲で任意に定めた値とする。それから、コピー先頭位置を個人識別子ＯＩＤの先頭から距離p_iに設定し、終端位置を$p_i + l_i$に設定するというようにコピー範囲を設定する。次に、図７３（ａ），（ｂ）に示すように、ペースト先頭位置を仮の役割識別子ＡＩＤの先頭から距離p_iに設定し、終端位置を$p_i + l_i$に設定するというようにペースト位置を設定する。

【０３８２】

それから、図７３（ａ），（ｂ）に示すように、上述したコピー範囲の文字列を仮の役割識別子ＡＩＤの上述したペースト位置に上書きして複写する（ステップＳ９１５）。このように上書きした文字列の特定の位置に位置情報p_iおよびl_iの値を、ＣＡが定めた方法で暗号化して、図７３（ｃ）で指定した位置に付加し（ステップＳ９１７）、更にこの位置情報を付加した文字列にセキュア・コミュニケーション・サービスＳＣＳのホストＯＩＤ（ホスト名、ドメイン名、またはＩＰアドレス）を図７３（ｃ）に示すように付加し（ステップＳ９１９）、更に図７３（ｃ）に示すようにリンク情報を付加する（ステップＳ９２０）。そして、このようにセキュア・コミュニケーション・サービスＳＣＳのホストＯＩＤおよびリンク情報を付加した文字列に認証局ＣＡのＯＩＤ秘密鍵で電子署名を施す（ステップＳ９２１）。

【０３８３】

次に、役割識別子ＡＩＤによる個人情報の登録および検索について説明する。アノニマス・ディレクトリ・サービスＡＤＳ７において、個人情報を登録するまでの流れを図７４（ａ）に示すが、この処理は図１１（ａ）で行ったものと同じである。

【０３８４】

また、アノニマス・ディレクトリ・サービスＡＤＳ７における検索処理は、図７４（ｂ）に示すように、検索者であるユーザＡが、自らの役割識別子ＡＩＤと例えば性別、年齢、趣味といったプライバシー情報からなる検索条件をアノニマス・ディレクトリ・サービスＡＤＳ７に送信する。アノニマス・ディレクトリ・サービスＡＤＳ７は、これらの情報を受信すると、検索条件にマッチした登録者の役割識別子ＡＩＤを抽出する。アノニマス・ディレクトリ・サービスＡＤＳ７は最後に検索者の役割識別子ＡＩＤと検索条件にマッチした登録者の役割識別子ＡＩＤのそれぞれのリンク情報から個別化アクセスチケットＰＡＴを生成し、検索者であるユーザＡ３に交付する。

【０３８５】

個別化アクセスチケットの生成は、アノニマス・ディレクトリ・サービスＡＤ

Ｓ７の検索結果として生成する。

【０３８６】

次に、図７５のフローチャートを参照して、ＡＤＳにおけるＰＡＴ生成処理について説明する。この図７５に示すＰＡＴ生成処理は、図１２で説明した処理においてステップＳ１２１５における処理を図７５のステップＳ１２１６で示すようにステップＳ１２１１で認証済みの検索者ＡＩＤのリンク情報を、登録者ＡＩＤ（ＡＤＳ登録時に登録者ＡＩＤの秘密鍵で認証済み）のリンク情報と連結するというように変更した点が異なるのみでその他の処理は同じである。なお、このステップＳ１２１６で連結した検索者ＡＩＤのリンク情報と登録者ＡＩＤのリンク情報からなる文字列に、登録者によりあらかじめ設定された移動制御フラグと有効期限を設定し、更に発信者フラグを「０」と設定する（ステップＳ１２１７）。

【０３８７】

次に、リンク指定型１対１個別化アクセスチケットＰＡＴによる移転制御について説明する。移転制御は、発信者番号通知のために行われるが、この発信者番号通知とは、着信者が発信者の役割識別子ＡＩＤと実際の発信者を対応付けられるようにすることである。

【０３８８】

アノニマス・ディレクトリ・サービスＡＤＳ７および着信者は、個別化アクセスチケットＰＡＴの移転制御フラグを設定することにより、発信者に番号通知させるか否かを選択させることができる。

【０３８９】

移転制御フラグを「１」に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５で移転制御が行われるため、着信者は発信者の役割識別子ＡＩＤと実際の発信者を対応付けることができる（発信者番号通知）。また、移転制御フラグを「０」に設定した場合には、着信者は発信者の役割識別子ＡＩＤと実際の発信者を対応付けることができない（発信者番号非通知）。

【０３９０】

図７７のフローチャートを参照して、ＳＣＳにおけるメール接続制御の処理手

順について説明する。この処理は図１４のステップＳ１４１９，Ｓ１４２１の処理における発信者ＡＩＤを図７７のステップＳ１４２０，Ｓ１４２２にそれぞれ示すように発信者ＡＩＤのリンク情報に変更する点が異なるのみであり、その他の処理は同じである。

【０３９１】

１．メールを入力する（ステップＳ１４１１）。

【０３９２】

２．ステップＳ１４１１で入力したメールのＴｏ：フィールドからＰＡＴを抽出する。次に、このＰＡＴに対するＡＤＳ公開鍵をＡＤＳに何らかの手段で問い合わせ、そのＡＤＳ公開鍵を取得する。そして、ＰＡＴをＡＤＳ公開鍵で認証する（ステップＳ１４１３）。

【０３９３】

３．ステップＳ１４１３における認証の結果

・ＰＡＴが改竄されている場合、ステップＳ１４１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する（ステップＳ１４２９）。

【０３９４】

・ＰＡＴが改竄されていない場合、ステップＳ１４１７に進む。

【０３９５】

４．ステップＳ１４１１のメールのＦｒｏｍ：フィールドから発信者ＡＩＤを抽出する。また、メールのＴｏ：フィールドのＰＡＴの移転制御フラグを解析し、ＰＡＴから発信者ＡＩＤのリンク情報を抽出する（ステップＳ１４１７，Ｓ１４２０）。

【０３９６】

５．ステップＳ１４１７，Ｓ１４２０で抽出した発信者ＡＩＤのリンク情報同士を比較する（ステップＳ１４２２）。

【０３９７】

６．ステップＳ１４２２における比較の結果

・両者が一致しない場合ステップＳ１４１１のメールを、メールのＦｒｏｍ：

フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する（ステップＳ１４２９）。

【０３９８】

・両者が一致する場合、ステップＳ１４２５に進む。

【０３９９】

７．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴから有効期限を抽出する（ステップＳ１４２５）。

【０４００】

８．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴが有効期限内かどうかを検証する（ステップＳ１４２７）。

【０４０１】

９．ステップＳ１４２７における検証の結果

・有効期限を過ぎている場合、ステップＳ１４１１のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する（ステップＳ１４２９）。

【０４０２】

・有効期限内の場合、ステップＳ１４３１に進む。

【０４０３】

１０．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴから移転制御フラグ値を調べる。

【０４０４】

１１．ステップＳ１４１１のメールのＴｏ：フィールドのＰＡＴから移転制御フラグ値を抽出する（ステップＳ１４３１）。

【０４０５】

１２．ステップＳ１４３１における抽出の結果

・移転制御フラグ値が「１」の場合、図１５～図１７の手順に従い、移転制御を行ってから（ステップＳ１４３５）、図７８の手順に従い、メールを着信者ＡＩＤ宛に転送する（ステップＳ１４３７）。

【０４０６】

・移転制御フラグ値が「０」の場合、図７８の手順に従い、メールを着信者ＡＩＤ宛に転送する（ステップＳ１４３７）。

【０４０７】

移転制御は、図１５～図１７を参照して説明したとおりである。

【０４０８】

次に、図７８のフローチャートを参照して接続制御について説明する。この接続制御は、図１８の処理においてステップＳ１８１１を図７８のステップＳ１８１０のように変更し、図１８のステップＳ１８１１とＳ１８１３の間に図７８のステップＳ１８５１，Ｓ１８５３を追加したものである。

【０４０９】

１．メールのＴｏ：フィールドのＰＡＴから、発信者ＡＩＤのリンク情報と着信者ＡＩＤのリンク情報を抽出する（ステップＳ１８１０）。この抽出したリンク情報をすべてＣＡに提示して、発信者ＡＩＤと着信者ＡＩＤを取得し（ステップＳ１８５１）、この取得したすべてのＡＩＤから、ＳＣＳホストＯＩＤを抽出する（ステップＳ１８５３）。

【０４１０】

２．この抽出した発信者、着信者それぞれのＳＣＳホストＯＩＤのデータ形式を調べる（ステップＳ１８１３）。

【０４１１】

３．ステップＳ１８１３における調査の結果

・発信者ＳＣＳホストＯＩＤと着信者ＳＣＳホストＯＩＤのうち、少なくとも一方がホスト名もしくはドメイン名で与えられている場合には、ステップＳ１８１５に進み、ホスト名またはドメイン名で与えられているＳＣＳホストＯＩＤをＤＮＳ(Domain Name Service) に問い合わせ、そのホスト名またはドメイン名に対するＩＰアドレスを取得してから、ステップＳ１８１７に進む。

【０４１２】

・発信者ＳＣＳホストＯＩＤと着信者ＳＣＳホストＯＩＤがともにＩＰアドレスで与えられている場合には、そのままステップＳ１８１７に進む。

【０４１３】

４．ステップＳ１８１５，Ｓ１８１７で抽出あるいは変換したＩＰアドレスを比較する（ステップＳ１８１７）。

【０４１４】

５．ステップＳ１８１７における比較の結果

・発信者ＳＣＳホストＯＩＤ（ＩＰアドレス）と着信者ＳＣＳホストＯＩＤ（ＩＰアドレス）が一致する場合、ステップＳ１８１９からステップＳ１８２３に進み、発信者ＡＩＤをアカウントに持つＳＣＳホスト上で、着信者ＡＩＤを検索する（ステップＳ１８２３）。この検索の結果、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在しない場合、ステップＳ１８２５からステップＳ１８２７に進み、ステップＳ１８１０のメールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【０４１５】

また、ステップＳ１８２５において、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在する場合、着信者ＡＩＤを検索条件として、着信拒否データベースに問い合わせる（ステップＳ１８２９）。

【０４１６】

この問い合わせの結果、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されている場合、ステップＳ１８３１からステップＳ１８２７に進み、メールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【０４１７】

また、ステップＳ１８３１において、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されていない場合、メールを、着信者のメールボックスまたはスプールに格納して正常終了する（ステップＳ１８３３）。

【０４１８】

一方、ステップＳ１８１９において、発信者ＳＣＳホストＯＩＤ（ＩＰアドレス）と着信者ＳＣＳホストＯＩＤ（ＩＰアドレス）が一致しない場合について説明する。

【０４１９】

まず、ＳＭＴＰに従い、メールを着信者ＡＩＤをアカウントに持つＳＣＳホストに転送する（ステップＳ１８３５）。

【０４２０】

次に、着信者ＡＩＤをアカウントに持つＳＣＳホスト上で、着信者ＡＩＤを検索する（ステップＳ１８３７）。

【０４２１】

この検索の結果、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在しない場合、ステップＳ１８３９からステップＳ１８４１に進み、メールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【０４２２】

また、ステップＳ１８３９において、着信者ＡＩＤのアカウントが、発信者ＡＩＤをアカウントに持つＳＣＳホスト上に存在する場合、ステップＳ１８４３に進む。ステップＳ１８４３では着信者ＡＩＤを検索条件として、着信拒否データベースに問い合わせる。

【０４２３】

ステップＳ１８４３における問い合わせの結果、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登録されている場合、ステップＳ１８４５からステップＳ１８４１に進み、メールを、メールのＦｒｏｍ：フィールドに記述された発信者ＡＩＤ宛に返信して、処理を中止する。

【０４２４】

また、ステップＳ１８４５において、メールのＴｏ：フィールドのＰＡＴ、または、発信者ＡＩＤに含まれるＳＣＳホストＯＩＤが着信拒否データベースに登

録されていない場合、ステップＳ１８４７に進み、メールを、着信者のメールボックスまたはスプールに格納して正常終了する。

【０４２５】

ＳＣＳにおけるメール返信処理は、図１９で説明した処理と同じである。

【０４２６】

次に、個別化アクセスチケットＰＡＴに対する着信拒否について説明する。着信者ＡＩＤ側で指定した個別化アクセスチケットＰＡＴがＴｏ：フィールドに記述されたメールが、着信者ＡＩＤに含まれるホストＯＩＤのセキュア・コミュニケーション・サービスＳＣＳ５に到着した場合には、そのセキュア・コミュニケーション・サービスＳＣＳ５はそのメールを着信者のメールボックスまたはスプールには格納せず、発信者ＡＩＤ宛に返信する。この一連の処理を着信拒否と呼ぶ。

【０４２７】

ユーザにおける着信拒否申請処理は、図２２に示すフローチャートを参照した説明と同じである。

【０４２８】

セキュア・コミュニケーション・サービスＳＣＳ５における着信拒否設定処理は、図２３を参照した説明と同じである。

【０４２９】

図７９のフローチャートおよび図８０を参照して、同一性の判定について説明する。

【０４３０】

１．変数$ＯＩＤ_{M}$の初期値を、ＯＩＤの全長Ｌと等しい長さで、かつ、すべての値が０であるビット列と定義する。また、変数$ＯＩＤ_{V}$の初期値を、ＯＩＤの全長Ｌと等しい長さで、かつ、すべての値が０であるビット列と定義する（ステップＳ２５１１）。

【０４３１】

２．処理対象のＡＩＤの集合から１個のＡＩＤを選択し、以下のビット演算を実行する（ステップＳ２５１３）。

【０４３２】

(a) ＡＩＤに含まれる位置情報をもとにして、変数AID_Mと変数AID_Vの値を決定する（ステップＳ２５１５）。ここで、

・AID_MはＯＩＤの全長Ｌと等しい長さで、かつ、

－ＯＩＤ情報が定義されている位置の値は１である。

【０４３３】

－ＯＩＤ情報が定義されていない位置の値は０である。

【０４３４】

ビット列と定義する（図８０）。

【０４３５】

・AID_VはＯＩＤの全長Ｌと等しい長さで、かつ、

－ＯＩＤ情報が定義されている位置の値はＯＩＤ情報の実際の値である

－ＯＩＤ情報が定義されていない位置の値は０である

ビット列と定義する（図８０）。

【０４３６】

(b) OID_MとAID_MのＡＮＤ演算を実行し、その結果を変数OVR_Mに代入する（ステップＳ２５１７）。

【０４３７】

(c) OVR_MとAID_MのＡＮＤ演算と、OVR_MとOID_MのＡＮＤ演算を実行し、その演算結果を比較する（ステップＳ２５１９）。

【０４３８】

・一致する場合OID_MとAID_MのＯＲ演算を実行し、実行結果をOID_Mに代入する（ステップＳ２５２１）。また、OID_VとAID_VのＯＲ演算を実行し、実行結果をOID_Mに代入する（ステップＳ２５２３）。

【０４３９】

・一致しない場合、ステップＳ２５２５に進み、実行する。

【０４４０】

(d) 処理対象のＡＩＤの集合から、次に処理するＡＩＤを抽出する。

【０４４１】

・集合に少なくとも１個のＡＩＤが含まれている場合、ステップＳ２５１９を実行する。

【０４４２】

・集合にＡＩＤが１個も含まれていない場合、ステップＳ２５２７に進む。

【０４４３】

(e) OID_M およびOID_V の値を出力する（ステップＳ２５２７）。

【０４４４】

最終的に得られたOID_M の値は、処理対象のＡＩＤの集合から復元できたＯＩＤ情報のすべての位置を表している。また、最終的に得られたOID_V の値は、処理対象のＡＩＤの集合から復元できたＯＩＤ情報のすべてを表している。つまり、OID_M とOID_V の値を用いると、

(a) OID_V の値を検索条件とすると、確率的にではあるがＯＩＤを求めることができる。

【０４４５】

(b) 上記検索の精度を、ＯＩＤ全長Ｌとの比OID_M Ｌで定量的に評価することができる。

【０４４６】

上述したように、本実施形態では、ユーザは、氏名、電話番号、電子メールアドレスといった情報を含む個人識別子ＯＩＤからこれらの情報を隠蔽した役割識別子ＡＩＤを作成すべく役割識別子ＡＩＤ請求メッセージを作成し、認証局ＣＡ１に送信すると、認証局ＣＡ１は、該メッセージを受け取って、リンク情報付き役割識別子ＡＩＤを生成し、ユーザに交付する。

【０４４７】

ユーザは、この交付されたリンク情報付き役割識別子ＡＩＤおよび性別、年齢、趣味等の個人情報をアノニマス・ディレクトリ・サービスＡＤＳ７に送信し、アノニマス・ディレクトリ・サービスＡＤＳ７にリンク情報付き役割識別子ＡＩＤと個人情報を登録する。このように登録された情報を検索する場合は、検索者は自己のリンク情報付き役割識別子ＡＩＤと検索条件（性別、年齢、趣味等のプ

ライバシー情報）をアノニマス・ディレクトリ・サービスＡＤＳ７に送信する。アノニマス・ディレクトリ・サービスＡＤＳ７は、これらの情報を受信すると、該検索条件にマッチした登録者のリンク情報付き役割識別子ＡＩＤを抽出する。そして、アノニマス・ディレクトリ・サービスＡＤＳ７は、検索者のリンク情報付き役割識別子ＡＩＤと検索条件にマッチした登録者のリンク情報付き役割識別子ＡＩＤからリンク指定型１対１個別化アクセスチケットＰＡＴを生成し、検索者に交付する。

【０４４８】

このリンク指定型１対１個別化アクセスチケットＰＡＴには、図７１（ｃ）に示すように発信者フラグ、移転制御フラグ、有効期限の値が設定されるが、この有効期限を着信者側で設定することにより、発信者からの接続を制限することができる。

【０４４９】

また、移転制御フラグの設定内容により発信者に番号通知させるか否かを、すなわち着信者が発信者ＡＩＤと実際の発信者を対応づけられるようにすることができるか否かを選択することができる。すなわち、移転制御フラグを１に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５で移転制御が行われ、着信者は発信者ＡＩＤと実際の発信者を対応付けることができる（発信者番号通知）。また、該フラグを０に設定した場合は、移転制御は行われず、着信者は発信者ＡＩＤと実際の発信者を対応付けることはできない（発信者番号非通知）。

【０４５０】

また、リンク指定型１対１個別化アクセスチケットＰＡＴで着信者を指定した呼をリンク指定型１対１個別化アクセスチケットＰＡＴのリンク情報で特定した着信者役割識別子ＡＩＤまたは発信者役割識別子ＡＩＤに着信するように、通信網に対して接続要求をすることができる。更に、リンク指定型１対１個別化アクセスチケットＰＡＴで指定した呼のうち、着信者が選択したリンク指定型１対１個別化アクセスチケットＰＡＴの呼を着信拒否することができる。また更に、匿名性を悪用し複数の発信者役割識別子ＡＩＤで個人攻撃を繰り返す発信者への対

処として、それら複数の発信者役割識別子ＡＩＤから個人識別子ＯＩＤの同一性を判定することができ、かつ、その個人識別子をある確率で取り出すことができる。

【０４５１】

次に、本発明の第７の実施形態に係る接続制御方法について図８１乃至図１０１を参照して説明する。上述した第６の実施形態では発信者と着信者を１対１に対応させるとともに、偽装防止のためにユーザ要求に基づいたリンク指定型１対１個別化アクセスチケットの新規生成、内容変更を許可していない場合について説明したのに対して、第７の実施形態では、上述した第２の実施形態と同様に、発信者と着信者を１対Ｎに対応させるとともに、リンク指定型１対Ｎ個別化アクセスチケットの新規生成、内容変更をユーザ主導で可能とする場合について説明するものである。なお、この発信者および着信者は所有者または会員である。

【０４５２】

第２の実施形態で説明したと同様に、グループ通信（メーリングリスト等）の会員構成は動的に変化するため、グループ通信の主催者は会員の電話番号、電子メールアドレス、インターネットメールアドレス等の連絡先情報を管理する必要がある。これに対して、第６の実施形態のように、リンク指定型１対１個別化アクセスチケットの新規生成、内容変更ができない場合には、連絡先情報の管理が困難である。例えば、グループを一体として管理することが困難であり、また移転制御のため、他の人に渡しても、メーリングリスト等グループ通信のアドレスとして機能しない。

【０４５３】

本第７の実施形態では、このような不具合を解消するためにリンク指定型１対Ｎ個別化アクセスチケットＰＡＴの新規生成および既存のリンク指定型１対Ｎ個別化アクセスチケットＰＡＴの内容変更をユーザ主導でできるようにしている。

【０４５４】

まず、本第７の実施形態で使用される各識別子の定義について図８１、図８２を参照して説明する。

【０４５５】

個人識別子（Official Identification ：ＯＩＤ）は、図８１（ａ）に示すように、認証局（Certificate Authority ：ＣＡ）が任意に生成した文字列（電話番号、電子メールアドレス等）、または前記文字列に対しＣＡ秘密鍵で電子署名を施したものである。

【０４５６】

リンク情報付き役割識別子（Anonymous Identification：ＡＩＤ）は、図８１（ｂ）に示すように、ＯＩＤの一部分とその位置情報、任意に生成した冗長な文字列、ＳＣＳのホストＯＩＤ、およびリンク情報からなる文字列に対し、ＣＡ秘密鍵で電子署名を施したものである。また、ＡＩＤはＳＣＳやＣＡで暗号化する場合もある。なお、リンク情報は、第６の実施形態のものと同じである。

【０４５７】

リンク指定型１対Ｎ個別化アクセスチケット（Personalized Access Ticket：ＰＡＴ）は、図８１（ｃ）に示すように、１個の所有者ＡＩＤ（HolderＡＩＤ）のリンク情報、１個以上の会員ＡＩＤ（MemberＡＩＤ）のリンク情報、発信者インデックス、所有者インデックス、有効期限情報、移転制御情報、ＰＡＴ演算装置識別子から構成されるリストに対し、ＰＡＴ演算装置識別子の秘密鍵で署名したものである。ここで、発信者インデックスは、ＡＩＤのリンク情報のリスト中の発信者ＡＩＤのリンク情報の位置を表す数値データで、先頭ＡＩＤが発信者ＡＩＤであれば１、２番目ならば２，…、ｎ番目ならばｎである。所有者インデックスは、ＡＩＤのリンク情報のリスト中の所有者ＡＩＤのリンク情報の位置を表す数値データで、先頭ＡＩＤが所有者ＡＩＤであれば１、２番目ならば２，…、ｎ番目ならばｎであると定義する。移転制御情報は、移転可の場合は「０」という数値、また移転不可の場合は「１」という数値のいずれかで表す。

【０４５８】

所有者ＡＩＤのリンク情報は、ＡＩＤリンク情報リスト中の所有者インデックスで指定した位置に書き込まれているＡＩＤリンク情報である。会員ＡＩＤのリンク情報は、所有者ＡＩＤリンク情報以外のすべてのＡＩＤリンク情報である。有効期限情報は、数値データであって、使用可能回数、ＰＡＴが利用不可能にな

る絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になる絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になってから利用不可能になるまでの相対時間（寿命）のいずれか、または複数を組み合わせて記述する。ＰＡＴ演算装置識別子は、ＰＡＴ演算装置のシリアルナンバーである。ＰＡＴ演算装置の秘密鍵は、上記シリアルナンバーに対する秘密鍵である。これらの中で、所有者ＡＩＤリンク情報と会員ＡＩＤリンク情報からなる部分を以後、ＡＩＤリストと呼ぶことにする。

【０４５９】

また、本第７の実施形態では、所有者役割識別子ＡＩＤに対応した識別子として、Enabler を導入している。Enabler は、図８２に示すように、Enabler であることを通信網上で一意に表す文字列とＡＩＤからなる文字列に対して、ＣＡ秘密鍵で電子署名したものである。

【０４６０】

次にＰＡＴの新規生成および内容変更における操作について説明する。通信端末上のセキュアなＰＡＴ演算装置、ＣＡ上もしくはＣＡから正当に依頼されたネットワーク上のＰＡＴ演算オブジェクト（以後、これもＰＡＴ演算装置と呼ぶことにする）において、次の操作が定義されるが、これは第２の実施形態のものと同じであり、図３３～図３６を参照して説明する。

【０４６１】

(1) ＡＩＤリストの演算：

所有者ＡＩＤおよび所有者ＡＩＤに対応するEnabler を用いて、ＡＩＤリストを新規生成あるいは変更する。

【０４６２】

(2) 有効期限情報および移転制御情報の設定：

所有者ＡＩＤおよび所有者ＡＩＤに対応するEnabler を用いて、有効期限情報および移転制御情報を設定もしくは変更する。

【０４６３】

所有者ＡＩＤに対してのみＡＩＤリストの演算を許可するために、以下の演算規則を定義する。

【０４６４】

(1) 新規生成（MakePAT）（図３３参照）：

ＡＩＤリスト（ＡＬＩＳＴ＜所有者ＡＩＤ｜会員AID_1，会員AID_2，…，会員AID_n＞）を新規生成し、生成後のＡＬＩＳＴに対し、有効期限情報および移転制御情報を設定する。

【０４６５】

【数４０】

$$AID_A + AID_B + \text{Enabler of } AID_B + \text{Enabler of } AID_A$$
$$\rightarrow ALIST<AID_A \mid AID_B > ALIST<AID_A \mid AID_B >$$
$$+ \text{Enabler of } AID_A + \text{有効期限情報} + \text{移転制御情報}$$
$$\rightarrow PAT<AID_A \mid AID_B >$$

(2) マージ（Merge ＰＡＴ）（図３４参照）：

同一所有者ＡＩＤの複数ＡＬＩＳＴをマージし、マージ後のＡＬＩＴＳに対し、有効期限情報および移転制御情報を設定する。

【０４６６】

【数４１】

$$ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots>$$
$$+ ALIST<AID_A \mid AID_{C1}, AID_{C2}, \cdots>$$
$$+ \text{Enabler of } AID_A$$
$$\rightarrow ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots, AID_{C1}, AID_{C2}, \cdots>$$
$$ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots, AID_{C1}, AID_{C2}, \cdots>$$
$$+ \text{Enabler of } AID_A + \text{有効期限情報} + \text{移転制御情報}$$
$$\rightarrow PAT<AID_A \mid AID_{B1}, AID_{B2}, \cdots, AID_{C1}, AID_{C2}, \cdots>$$

(3) 分割（Split ＰＡＴ）（図３５参照）：

ＡＬＩＳＴを同一所有者ＡＩＤの複数ＡＬＩＳＴに分解し、分解後のすべてのＡＬＩＳＴに対し、それぞれ、有効期限情報および移転制御情報を設定する。

【数４２】

$$ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots, AID_{C1}, AID_{C2}, \cdots> + Enabler_A$$
$$\rightarrow ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots> + ALIST<AID_A \mid AID_{C1}, AID_{C2}, \cdots>$$
$$ALIST<AID_A \mid AID_{C1}, AID_{C2}, \cdots> + \text{Enabler of } AID_A + \text{有効期限情報} + \text{移転制御情報}$$
$$\rightarrow PAT<AID_A \mid AID_{C1}, AID_{C2}, \cdots>$$

(4) 所有者変更（Trans ＰＡＴ）（図３６参照）：

ＡＬＩＴＳの所有者ＡＩＤを変更し、変更後のＡＬＩＳＴに対し有効期限情報および移転制御情報を設定する。

【０４６７】

【数４３】

$$ALIST<AID_A \mid AID_B> + ALIST<AID_A \mid AID_{C1}, AID_{C2}, \cdots> + \text{Enabler of } AID_A + \text{Enabler of } AID_B$$
$$\rightarrow ALIST<AID_B \mid AID_{C1}, AID_{C2}, \cdots>$$
$$ALIST<AID_B \mid AID_{C1}, AID_{C2}, \cdots> + \text{Enabler of } AID_B + \text{有効期限情報} + \text{移転制御情報}$$
$$\rightarrow PAT<AID_B \mid AID_{C1}, AID_{C2}, \cdots>$$

有効期限情報の設定における操作では、所有者ＡＩＤとこれに対応したEnabler の両者を所有するユーザにのみ有効期限情報の設定を許可するために、以下の操作を定義する。

【０４６８】

【数４４】

$$ALIST<AID_A \mid AID_B> + \text{Enabler of } A + \text{有効期限情報} \rightarrow PAT<AID_A \mid AID_B>$$

移転制御情報の設定における操作では、所有者ＡＩＤとこれに対応したEnabler の両者を所有するユーザにのみ移転制御情報の設定を許可するために、以下の操作を定義する。

【０４６９】

【数４５】

$$ALIST<AID_A \mid AID_B> + \text{Enabler of } A + \text{移転制御情報} \rightarrow PAT<AID_A \mid AID_B>$$

次に、本実施形態の全体構成を示す図８３～図８９について説明する。図８３～図８９において、通信網からAID_Aを割り当てられたユーザＡは、ユーザＡの計算機にAID_Aおよび Enabler of AID_Aを保存し、フロッピードライブ、ＣＤ－ＲＯＭドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、上記仕様と同等の機能を持つ通信端末（電話、携帯電話等）に、AID_Aおよび Enabler of AID_Aを保存している。

【０４７０】

同様に、通信網からAID_Bを割り当てられたユーザＢは、自らの計算機にAID_Bおよび Enabler of AID_Bを保存し、フロッピードライブ、ＣＤ－ＲＯＭドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、上記仕様と同等の機能を持つ通信端末（電話、携帯電話等）に、AID_Aおよび Enabler of AID_Aを保存している。

【０４７１】

以下、ユーザＡがＰＡＴ＜リンク（AID_A）｜リンク（AID_B）＞を生成する手順を説明する。

【０４７２】

(1) ユーザＡは、以下の手段のいずれかを用いて、AID_Bおよび Enabler of AID_Bを取得する。

【０４７３】

・オンライン検索サービスにAID_Bと Enabler of AID_Bを登録し、ユーザＡが検索結果として取得するのを待つ（図８３）。

【０４７４】

・電子メール、シグナリング等でAID_Bと Enabler of AID_BをユーザＡに直接送信する（図８４～図８５）。

【０４７５】

・フロッピーディスク、ＣＤ－ＲＯＭ、ＭＯ、ＩＣカード等の磁気、光、電子メディアにAID_B と Enabler of AID_B を蓄積し、ユーザＡに渡す。または、ユーザＡが閲覧して取得するのを待つ（図８６～図８７）。

【０４７６】

・書籍、名刺等の紙メディアにAID_B と Enabler of AID_B を記載し、ユーザＡに渡す（図８８～図８９）。もしくは、ユーザＡが閲覧し取得するのを待つ。

【０４７７】

(2) 上述した（１）のいずれかの手段でAID_B および Enabler of AID_B を取得したユーザＡは、ＰＡＴ演算装置に対しMakeＰＡＴ命令を発行する。この手順は図８３～図８９で共通で、以下の通りに定義する。

【０４７８】

(a) ユーザＡは、ユーザＡの通信端末にAID_A 、 Enabler of AID_A 、AID_B 、 Enabler of AID_B 、有効期限情報、および移転制御情報値をセットし、MakeＰＡＴ命令の発行を要求する。

【０４７９】

(b) ユーザＡの通信端末は、MakeＰＡＴ命令を生成する。

【０４８０】

(c) ユーザＡの通信端末は、生成したMakeＰＡＴ命令を電子メール、シグナリング等の手段でＰＡＴ演算装置に送信する（MakeＰＡＴ命令の発行）。

【０４８１】

(d) ＰＡＴ演算装置は、受信したMakeＰＡＴ命令を図４４、図９０、図９１、図９５に従って処理し、ＰＡＴ＜リンク（AID_A ）｜リンク（AID_B ）＞を生成する。具体的には、

【数４６】

$$AID_A + AID_B + \text{Enabler of } AID_B + \text{Enabler of } AID_A \rightarrow ALIST\langle AID_A \mid AID_B \rangle$$

$$ALIST\langle AID_A \mid AID_B \rangle + \text{Enabler of } AID_A$$

＋有効期限情報＋移転制御情報

→ＰＡＴ＜リンク（AID_A）｜リンク（AID_B）＞

(e) ＰＡＴ演算装置は、生成したＰＡＴ＜リンク（AID_A）｜リンク（AID_B）＞を電子メール、シグナリング等の手段でユーザＡの通信端末、または必要に応じて、ユーザＢの通信端末に送信する。

【０４８２】

(f) ユーザＡ（またはユーザＢ）の通信端末は、受信したＰＡＴ＜リンク（AID_A）｜リンク（AID_B）＞をユーザＡの通信端末の記憶装置に保存する。

【０４８３】

ＰＡＴのマージ（Merge ＰＡＴ、図４４、図９０、図９２、図９６）、ＰＡＴの分割（Split ＰＡＴ、図４５、図４６、図４９、図５３）、ＰＡＴの所有者変更（Trans ＰＡＴ、図４４、図９０、図９４、図９８）も同様の手順である。

【０４８４】

次に、MakeＰＡＴ、Merge ＰＡＴ、Trans ＰＡＴの処理の全体の流れを図４４に従って説明する。

【０４８５】

１．新規生成または変更後のＰＡＴの所有者ＡＩＤを決定する（ステップＳ４４１１）。

【０４８６】

２．新規生成または変更後のＰＡＴの会員ＡＩＤを決定する（ステップＳ４４１２）。

【０４８７】

３．ステップＳ４４１１の所有者ＡＩＤとステップＳ４４１２の会員ＡＩＤを要素に持つＡＩＤリストを生成する（ステップＳ４４１３）。

【０４８８】

４．メッセージから有効期限情報および移転制御情報を抽出する（ステップＳ４４１４）。

【０４８９】

５．ステップＳ４４１３のＡＩＤリストに、ステップＳ４４１４の有効期限情報および移転制御情報を設定する（ステップＳ４４１５）。

【０４９０】

６．ステップＳ４４１５の結果に所有者インデックスを設定する（ステップＳ４４１６）。

【０４９１】

７．ステップＳ４４１６の結果にＰＡＴ演算装置の識別子（シリアルナンバー）を設定する（ステップＳ４４１７）。

【０４９２】

８．ステップＳ４４１７の結果にＰＡＴ演算装置の識別子（シリアルナンバー）の秘密鍵で署名する（ステップＳ４４１８）。

【０４９３】

９．ステップＳ４４１８の結果を所有者ＡＩＤ宛に送信し、必要に応じて会員ＡＩＤ宛にも送信する（ステップＳ４４１９）。

【０４９４】

Split ＰＡＴは、MakeＰＡＴ、Merge ＰＡＴ、Trans ＰＡＴとは異なり、複数のＰＡＴを生成する。従って、Split ＰＡＴの処理は図４５に示すように図４４の処理に再帰制御（ステップＳ４４２０）を加えることと定義する。

【０４９５】

次に、所有者ＡＩＤの決定について説明する。新規生成ＰＡＴまたは内容変更後ＰＡＴの所有者ＡＩＤの決定は、以下の手順に従う。

【０４９６】

MakeＰＡＴの場合、所有者ＡＩＤの決定は、図９１に示すように行われる。

【０４９７】

１．図５６のメッセージから新規生成ＰＡＴの所有者ＡＩＤにしたいＡＩＤを抽出する（ステップＳ４７１１）。

【０４９８】

２．上記ＡＩＤが存在する場合には、上記メッセージから、新規生成ＰＡＴの所

有者ＡＩＤにしたいＡＩＤのEnabler を抽出する（ステップＳ４７１２，Ｓ４７１３）。

【０４９９】

３．Enabler が存在する場合には、ステップＳ４７１１で抽出したＡＩＤについて、ステップＳ４７１３で抽出したEnabler と対応しているか調べる（ステップＳ４７１４，Ｓ４７１５）。

【０５００】

４．対応している場合には、抽出したＡＩＤのリンク情報を新規生成ＰＡＴの所有者ＡＩＤのリンク情報に決定し、対応していない場合には、処理を中止する（ステップＳ４７１６，Ｓ４７１８）。

【０５０１】

Merge ＰＡＴの場合、所有者ＡＩＤの決定は、図９２に示すように行われる。

【０５０２】

１．図９９のメッセージから、マージ対象のＰＡＴをすべて抽出する（ステップＳ４８１１）。

【０５０３】

２．ステップＳ４８１１で抽出したすべてのＰＡＴから、所有者ＡＩＤのリンク情報を抽出する（ステップＳ４８２０）。このリンク情報をＣＡに提示して所有者ＡＩＤを取得する（ステップＳ４８２２）。

【０５０４】

３．ステップＳ４８２２で取得した所有者ＡＩＤを比較し（ステップＳ４８１３）、少なくとも１個の所有者ＡＩＤが一致しない場合、処理を中止し、すべての所有者ＡＩＤが一致する場合、下記処理（ステップＳ４８１４）を実行する。

【０５０５】

４．図９９のメッセージから、マージ後ＰＡＴの所有者ＡＩＤにしたいＡＩＤのEnabler を抽出する（ステップＳ４８１４）。

【０５０６】

５．Enabler が存在する場合、ステップＳ４８１３で比較の結果のＡＩＤがステップＳ４８１４で抽出したEnabler と対応しているか調べ（ステップＳ４８１５

，Ｓ４８１６）、対応している場合、ステップＳ４８１１で抽出したＡＩＤのリンク情報をマージ後ＰＡＴの所有者ＡＩＤのリンク情報に決定し、対応していない場合、処理を中止する（ステップＳ４８１７，Ｓ４８２４）。

【０５０７】

Split ＰＡＴの場合、所有者ＡＩＤの決定は、図９３に示すように行われる。

【０５０８】

１．図１００のメッセージから、分割対象のＰＡＴを抽出する（ステップＳ４９１１）。

【０５０９】

２．ステップＳ４９１１で抽出したＰＡＴから、所有者ＡＩＤのリンク情報を抽出する（ステップＳ４９２１）。このリンク情報をＣＡに提示して、所有者ＡＩＤを取得する（ステップＳ４９２３）。

【０５１０】

３．図１００のメッセージから、分割後のすべてのＰＡＴの所有者ＡＩＤにしたいＡＩＤのEnabler を抽出する（ステップＳ４９１３）。

【０５１１】

４．Enabler が存在する場合、ステップＳ４９２３で取得したＡＩＤがステップＳ４９１３で抽出したEnabler と対応しているか調べ（ステップＳ４９１４，Ｓ４９１５，Ｓ４９１６）、対応している場合、ステップＳ４９１１で抽出したＡＩＤのリンク情報を分割後のすべてのＰＡＴの所有者ＡＩＤのリンク情報に決定し（ステップＳ４９２５）、対応していない場合、処理を中止する（ステップＳ４９１６）。

【０５１２】

Trans ＰＡＴの場合、所有者ＡＩＤの決定は、図９４に示すように行われる。

【０５１３】

１．図１０１のメッセージから、変更対象のＰＡＴを抽出する（ステップＳ５０１１）。

２．この抽出したＰＡＴから、（現在の）所有者ＡＩＤのリンク情報を抽出する（ステップＳ５０２５）。このリンク情報をＣＡに提示して、（現在）の所有者

ＡＩＤを取得する（ステップＳ５０２７）。

【０５１４】

３．図１０１のメッセージから、（現在の）所有者ＡＩＤのEnabler を抽出する（ステップＳ５０１３）。

４．Enabler が存在する場合、ステップＳ５０１２で抽出したＡＩＤがステップＳ５０１３で抽出したEnabler と対応しているか調べる（ステップＳ５０１４～Ｓ５０１６）。

【０５１５】

５．対応している場合、図１０１のメッセージから、新しく所有者ＡＩＤにしたいＡＩＤを抽出し、対応していない場合は処理を中止する（ステップＳ５０１７）。

【０５１６】

６．上記ＡＩＤが会員ＡＩＤである場合、上記メッセージから、新しく所有者ＡＩＤにしたいＡＩＤのEnabler を抽出する（ステップＳ５０１８，Ｓ５０１９）。

【０５１７】

７．Enabler が存在する場合、ステップＳ５０１７で抽出したＡＩＤがステップＳ５０１９で抽出したEnabler と対応しているか調べ（ステップＳ５０２０～Ｓ５０２２）、対応している場合ステップＳ５０１７で抽出したＡＩＤのリンク情報を変更後ＰＡＴの所有者ＡＩＤである新所有者ＡＩＤのリンク情報に決定し（ステップＳ５０２３）、対応していない場合、処理を中止する（ステップＳ５０２２）。

【０５１８】

次に、会員ＡＩＤの決定について説明する。新規生成ＰＡＴまたは内容変更後ＰＡＴの会員ＡＩＤの決定は、以下の手順に従う。

【０５１９】

MakeＰＡＴの場合、所有者ＡＩＤの決定は、図５１に示すように行われる。

【０５２０】

１．図５６のメッセージから、新規生成ＰＡＴの会員ＡＩＤにしたいＡＩＤをす

べて抽出する（ステップＳ５１１１）。

２．ＡＩＤが存在する場合には、図５６のメッセージから、新規生成ＰＡＴの会員ＡＩＤにしたいすべてのＡＩＤについて、それぞれEnabler を抽出する（ステップＳ５１１２，Ｓ５１１３）。

【０５２１】

３．Enabler が存在する場合、ステップＳ５１１１で抽出したすべてのＡＩＤについて、それぞれステップＳ５１１２で抽出したEnabler と対応しているか調べ（ステップＳ５１１４～Ｓ５１１６）、対応しているＡＩＤのリンク情報を新規生成ＰＡＴの会員ＡＩＤのリンク情報に決定し（ステップＳ５１１７）、対応していないＡＩＤを廃棄し、すべての処理対象ＡＩＤについて上記処理を繰り返し行う（ステップＳ５１１８）。

【０５２２】

Merge ＰＡＴの場合、会員ＡＩＤの決定は、図９６に示すように行われる。

【０５２３】

１．図９９のメッセージから、マージ対象のすべてのＰＡＴを抽出する（ステップＳ５２１１）。

２．この抽出したすべてのＰＡＴから、それぞれ（所有者インデックスをもとに）所有者ＡＩＤのリンク情報を抽出する（ステップＳ５２２１）。

【０５２４】

３．この抽出したすべての所有者ＡＩＤのリンク情報をマージ後ＰＡＴの所有者ＡＩＤのリンク情報と一致するか比較する（ステップＳ５２２３）。

【０５２５】

４．一致する場合には、ＰＡＴからすべての会員ＡＩＤのリンク情報を抽出し（ステップＳ５２２５）、この抽出した会員ＡＩＤのリンク情報をすべてマージ後の会員ＡＩＤのリンク情報に決定する（ステップＳ５２２７）。

【０５２６】

５．一致しない場合、ＰＡＴを削除し、処理対象を次のＰＡＴとして、上記処理を繰り返し行い、処理対象が存在しない場合には、処理を中止する（ステップＳ５２１６）。

【０５２７】

Split ＰＡＴの場合、会員ＡＩＤの決定は、図９７に示すように行われる。

【０５２８】

１．図１００のメッセージから分割対象のＰＡＴを抽出する（ステップＳ５３１１）。

２．この抽出したＰＡＴから所有者ＡＩＤのリンク情報を抽出する（ステップＳ５３２１）。

【０５２９】

３．この抽出したリンク情報を分割後ＰＡＴの所有者ＡＩＤのリンク情報と一致するか比較する（ステップＳ５３２３）。

【０５３０】

４．一致する場合には、メッセージから会員ＡＩＤのリストを抽出し（ステップＳ５３１４）、一致しない場合には、処理を中止する。

【０５３１】

５．ステップＳ５３１１のＰＡＴから、上記リストに含まれるすべての会員ＡＩＤのリンク情報を抽出する（ステップＳ５３２５）。

【０５３２】

６．この抽出した会員ＡＩＤのリンク情報をすべて、分割後の会員ＡＩＤのリンク情報に決定する（ステップＳ５３２７）。

【０５３３】

Trans ＰＡＴの場合、会員ＡＩＤの決定は、図９８に示すように行われる。

【０５３４】

１．図１０１のメッセージから所有者変更したいＰＡＴを抽出し、この抽出したＰＡＴからすべての会員ＡＩＤのリンク情報を抽出する（ステップＳ５４２１）。

【０５３５】

２．所有者ＡＩＤを変更後ＰＡＴの会員ＡＩＤにするかチェック（ステップＳ５４１２）、会員ＡＩＤにする場合には、ステップＳ５４２１のＰＡＴから所有者ＡＩＤのリンク情報も抽出する（ステップＳ５４２３）。

【０５３６】

３．残りのすべてのＡＩＤのリンク情報をすべて、変更後ＰＡＴの会員ＡＩＤのリンク情報に決定する（ステップＳ５４２５）。

【０５３７】

次に、ＡＩＤリストの生成について説明する。ＡＩＤリストの生成は、MakeＰＡＴ、Merge ＰＡＴ、Split ＰＡＴ、Trans ＰＡＴで共通であり、図９０に示すように行われる。

【０５３８】

１．会員ＡＩＤ数をもとに、ＡＩＤリストのバッファ長を決定する（ステップＳ４６１１）。

２．この決定した情報をもとに、バッファを生成する（ステップＳ４６１２）。

【０５３９】

３．所有者ＡＩＤのリンク情報をステップＳ４６１２のバッファの空き領域にコピーする（ステップＳ４６１７）。

４．会員ＡＩＤのリンク情報をステップＳ４６１７の残りの空き領域にコピーする（ステップＳ４６１８）。

【０５４０】

５．次の会員ＡＩＤが存在する場合には、ステップＳ４６１８に戻り、繰り返し行う（ステップＳ４６１５）。

【０５４１】

本実施形態の、Enabler の正当性の検証は図５５を参照した前述した説明と同じである。また、このEnabler の正当性の検証は、MakeＰＡＴ、Merge ＰＡＴ、Split ＰＡＴ、Trans ＰＡＴで共通である。

【０５４２】

【発明の効果】

以上説明したように、本発明によれば、付与情報をユーザに付与し、付与情報とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示す個別化アクセスチケットを発行し、発信者からの発信要求に対して個別化アクセスチケットを用いて

アクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うので、ユーザの本当の識別子を隠蔽しつつ、ユーザの特性を表す情報を公開し、この情報に基づいて適切な通信を行うことができ、従来のような第三者からの攻撃等を的確に防止することができる。加えて、着信者が匿名性を悪用した発信者による攻撃を受けた場合には、その攻撃による着信者への被害を最小限に食い止めることができる。

【０５４３】

また、本発明によれば、第１の個別化アクセスチケットの所有者役割識別子を第１の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第２の個別化アクセスチケット変更権(Enabler) 、役割識別子により新たな所有者役割識別子の変更、新たな会員役割識別子の追加または会員役割識別子の削除を行い、第２の個別化アクセスチケットを作成するので、個別化アクセスチケットの新規生成、変更をユーザ主導で行うことができ、例えば動的に変化するグループ通信（メーリングリスト等）の会員の連絡先情報等も適確に管理することができる。

【０５４４】

更に、本発明によれば、個別化アクセスチケット（ＰＡＴ）の新規生成および既存の個別化アクセスチケット（ＰＡＴ）の内容変更を行うために、Ｎｕｌｌ－ＡＩＤ（AID_{Null}）および該Ｎｕｌｌ－ＡＩＤの Enabler(Enabler of Ｎｕｌｌ－ＡＩＤまたは Enabler of AID_{Null}）を使用するので、会員ＡＩＤおよび Enabler of 会員ＡＩＤを所有者ＡＩＤに渡さなくても新規生成（MakeＰＡＴ）およびマージ（Merge ＰＡＴ）を行うことができるとともに、また会員ＡＩＤを用いた成りすましを防止することができる。

【０５４５】

本発明によれば、Ｎｕｌｌ－ＡＩＤは個別化アクセスチケット（ＰＡＴ）の所有者ＡＩＤとしてのみ使用可能であり、

【数４７】

$$PAT<AID_{Null} \mid AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$$

は許可し、また

【数４８】

$$PAT<AID_{所有者} \mid AID_{Null}, AID_{会員1}, AID_{会員2}, \cdots, AID_{会員N}>$$

は許可しないので、$PAT<AID_{所有者} \mid AID_{会員}>$の所有者が$AID_{会員}$のEnabler を知らない場合には、このＰＡＴから$PAT<AID_{Null} \mid AID_{会員}>$を作成することはできない。

【０５４６】

また、本発明によれば、Ｇｏｄ－ＡＩＤ（AID_{God}）を用いて、個別化アクセスチケット（ＰＡＴ）に読取専用属性を設定するので、グループ通信において参加者を固定することができる。

【０５４７】

更に、本発明によれば、役割識別子は該役割識別子を一意に特定するためのリンク情報を有し、該リンク情報を個別化アクセスチケットに設定し、該個別化アクセスチケットで使用される役割識別子を前記リンク情報で特定するので、個別化アクセスチケットは役割識別子の実体を含まないため、役割識別子の実体を使用することなく着信拒否機能を実現することができる。

【図面の簡単な説明】

【図１】

本発明において使用される役割識別子ＡＩＤ、個別化アクセスチケットＰＡＴを示す説明図である。

【図２】

本発明の一実施形態の全体構成図である。

【図３】

個人識別子ＯＩＤと役割識別子ＡＩＤの例を示している。

【図４】

ユーザが役割識別子ＡＩＤを認証局ＣＡに対して請求する処理を示すフローチャートである。

【図５】

役割識別子ＡＩＤの請求に対する認証局ＣＡが役割識別子ＡＩＤをユーザに対

して交付する処理を示すフローチャートである。

【図６】

ユーザにおけるＡＩＤ交付処理を示すフローチャートである。

【図７】

役割識別子ＡＩＤの請求メッセージの例を示す図である。

【図８】

役割識別子ＡＩＤの交付メッセージの例を示す図である。

【図９】

認証局ＣＡにおける役割識別子ＡＩＤの生成処理を示すフローチャートである。

【図１０】

図９のＡＩＤ生成処理に関連する説明図である。

【図１１】

アノニマス・ディレクトリ・サービスＡＤＳにおける役割識別子ＡＩＤの登録と個別化アクセスチケットＰＡＴの交付の例を示す説明図である。

【図１２】

ＡＤＳにおいて個別化アクセスチケットＰＡＴを生成する場合の処理を示すフローチャートである。

【図１３】

図１２のＰＡＴ生成処理に関連する説明図である。

【図１４】

ＳＣＳにおけるメール転送制御を示すフローチャートである。

【図１５】

ＳＣＳにおける移転制御を示すフローチャートである。

【図１６】

ユーザにおける移転制御を示すフローチャートである。

【図１７】

ＳＣＳにおける移転制御を示すフローチャートである。

【図１８】

ＳＣＳにおける個別化アクセスチケットＰＡＴに対する接続制御を示すフローチャートである。

【図１９】

ＳＣＳにおけるメール返信処理を示すフローチャートである。

【図２０】

ユーザ間の電子メールの例を示す図である。

【図２１】

着信拒否された場合の電子メールの例を示す図である。

【図２２】

ユーザにおける着信拒否申請処理を示すフローチャートである。

【図２３】

ＳＣＳにおける着信拒否設定処理を示すフローチャートである。

【図２４】

着信拒否申請メッセージおよび着信拒否通知メッセージの例を示す図である。

【図２５】

役割識別子ＡＩＤについて個人識別子ＯＩＤの同一性を判定する処理を示すフローチャートである。

【図２６】

図２５に示す同一性判定処理に関連する役割識別子ＡＩＤおよび個人識別子ＯＩＤの例を示す図である。

【図２７】

アナログ公衆網における二重番号登録を示す説明図である。

【図２８】

アナログ公衆網における発信者番号通知を示す説明図である。

【図２９】

デジタル携帯網およびアナログ公衆網における着信拒否を示す説明図である。

【図３０】

匿名電子メールの説明図である。

【図３１】

本発明の第２の実施形態に使用されるＯＩＤ，ＡＩＤ，ＰＡＴのデータ構造を示す図である。

【図３２】

本発明の第２の実施形態に使用されるEnabler のデータ構造を示す図である。

【図３３】

本発明の第２の実施形態に使用される演算規則（MakeＰＡＴ）の定義を示す図である。

【図３４】

本発明の第２の実施形態に使用される演算規則（Merge ＰＡＴ）の定義を示す図である。

【図３５】

本発明の第２の実施形態に使用される演算規則（Split ＰＡＴ）の定義を示す図である。

【図３６】

本発明の第２の実施形態に使用される演算規則（Trans ＰＡＴ）の定義を示す図である。

【図３７】

本発明の第２の実施形態に使用される装置構成（１）を示す図である。

【図３８】

本発明の第２の実施形態に使用される装置構成（２）を示す図である。

【図３９】

本発明の第２の実施形態に使用される装置構成（３）を示す図である。

【図４０】

本発明の第２の実施形態に使用される装置構成（４）を示す図である。

【図４１】

本発明の第２の実施形態に使用される装置構成（５）を示す図である。

【図４２】

本発明の第２の実施形態に使用される装置構成（６）を示す図である。

【図４３】

本発明の第２の実施形態に使用される装置構成（７）を示す図である。

【図４４】

本発明の第２の実施形態の処理全体の流れ（MakeＰＡＴ，Merge ＰＡＴ，Trans ＰＡＴ）を示すフローチャートである。

【図４５】

本発明の第２の実施形態の処理全体の流れ（Split ＰＡＴ）を示すフローチャートである。

【図４６】

本発明の第２の実施形態におけるＡＩＤリストの生成処理（MakeＰＡＴ，Merge ＰＡＴ，Split ＰＡＴ，Trans ＰＡＴ）を示すフローチャートである。

【図４７】

本発明の第２の実施形態における所有者ＡＩＤの決定処理（MakeＰＡＴ）を示すフローチャートである。

【図４８】

本発明の第２の実施形態における所有者ＡＩＤの決定処理（Merge ＰＡＴ）を示すフローチャートである。

【図４９】

本発明の第２の実施形態における所有者ＡＩＤの決定処理（Split ＰＡＴ）を示すフローチャートである。

【図５０】

本発明の第２の実施形態における所有者ＡＩＤの決定処理（Trans ＰＡＴ）を示すフローチャートである。

【図５１】

本発明の第２の実施形態における会員ＡＩＤの決定処理（MakeＰＡＴ）を示すフローチャートである。

【図５２】

本発明の第２の実施形態における会員ＡＩＤの決定処理（Merge ＰＡＴ）を示すフローチャートである。

【図５３】

本発明の第２の実施形態における会員ＡＩＤの決定処理（Split ＰＡＴ）を示すフローチャートである。

【図５４】

本発明の第２の実施形態における会員ＡＩＤの決定処理（Trans ＰＡＴ）を示すフローチャートである。

【図５５】

本発明の第２の実施形態におけるEnabler の正当性の検証処理（MakeＰＡＴ，Merge ＰＡＴ，Split ＰＡＴ，Trans ＰＡＴ）を示すフローチャートである。

【図５６】

本発明の第２の実施形態におけるMakeＰＡＴ命令を含むメッセージを示す図である。

【図５７】

本発明の第２の実施形態におけるMerge ＰＡＴ命令を含むメッセージを示す図である。

【図５８】

本発明の第２の実施形態におけるSplit ＰＡＴ命令を含むメッセージを示す図である。

【図５９】

本発明の第２の実施形態におけるTrans ＰＡＴ命令を含むメッセージを示す図である。

【図６０】

本発明の第２の実施形態の一元管理型メーリングリストへの適用例を示す図である。

【図６１】

本発明の第３の実施形態に使用されるＮｕｌｌ－ＡＩＤのデータ構造を示す図である。

【図６２】

本発明の第３の実施形態に使用される Enabler of Ｎｕｌｌ－ＡＩＤのデータ

構造を示す図である。

【図６３】

本発明の第３の実施形態の第１の応用例を示す図である。

【図６４】

本発明の第３の実施形態の第２の応用例を示す図である。

【図６５】

本発明の第４の実施形態に使用されるＧｏｄ－ＡＩＤのデータ構造を示す図である。

【図６６】

本発明の第４の実施形態におけるＧｏｄ－ＡＩＤ規則の処理を示すフローチャートである。

【図６７】

本発明の第４の実施形態の第１の応用例を示す図である。

【図６８】

本発明の第４の実施形態の第２の応用例を示す図である。

【図６９】

本発明の第５の実施形態における会員ＡＩＤのチェック処理を示すフローチャートである。

【図７０】

本発明の第６の実施形態の全体構成図である。

【図７１】

第６の実施形態に使用される個人識別子ＯＩＤ、リンク情報付き役割識別子ＡＩＤ、リンク指定型１対１個別化アクセスチケットＰＡＴの例を示している。

【図７２】

認証局ＣＡにおける役割識別子ＡＩＤの生成処理を示すフローチャートである。

【図７３】

図７２のＡＩＤ生成処理に関連する説明図である。

【図７４】

アノニマス・ディレクトリ・サービスＡＤＳにおける役割識別子ＡＩＤの登録と個別化アクセスチケットＰＡＴの交付の例を示す説明図である。

【図７５】

ＡＤＳにおいてリンク指定型１対１個別化アクセスチケットＰＡＴを生成する場合の処理を示すフローチャートである。

【図７６】

図７５のＰＡＴ生成処理に関連する説明図である。

【図７７】

ＳＣＳにおけるメール転送制御を示すフローチャートである。

【図７８】

ＳＣＳにおけるリンク指定型１対１個別化アクセスチケットＰＡＴに対する経路制御を示すフローチャートである。

【図７９】

リンク情報付き役割識別子ＡＩＤについて個人識別子ＯＩＤの同一性を判定する処理を示すフローチャートである。

【図８０】

図７９に示す同一性判定処理に関連するリンク情報付き役割識別子ＡＩＤおよび個人識別子ＯＩＤの例を示す図である。

【図８１】

本発明の第７の実施形態に使用される個人識別子ＯＩＤ、リンク情報付き役割識別子ＡＩＤ、リンク指定型１対Ｎ個別化アクセスチケットＰＡＴのデータ構造を示す図である。

【図８２】

本発明の第７の実施形態に使用されるEnabler のデータ構造を示す図である。

【図８３】

本発明の第７の実施形態に使用される装置構成（１）を示す図である。

【図８４】

本発明の第７の実施形態に使用される装置構成（２）を示す図である。

【図８５】

本発明の第７の実施形態に使用される装置構成（３）を示す図である。

【図８６】

本発明の第７の実施形態に使用される装置構成（４）を示す図である。

【図８７】

本発明の第７の実施形態に使用される装置構成（５）を示す図である。

【図８８】

本発明の第７の実施形態に使用される装置構成（６）を示す図である。

【図８９】

本発明の第７の実施形態に使用される装置構成（７）を示す図である。

【図９０】

本発明の第７の実施形態におけるＡＩＤリストの生成処理（MakeＰＡＴ，Merge ＰＡＴ，Split ＰＡＴ，Trans ＰＡＴ）を示すフローチャートである。

【図９１】

本発明の第７の実施形態における所有者ＡＩＤの決定処理（Merge ＰＡＴ）を示すフローチャートである。

【図９２】

本発明の第７の実施形態における所有者ＡＩＤの決定処理（MakeＰＡＴ）を示すフローチャートである。

【図９３】

本発明の第７の実施形態における所有者ＡＩＤの決定処理（Split ＰＡＴ）を示すフローチャートである。

【図９４】

本発明の第７の実施形態における所有者ＡＩＤの決定処理（Trans ＰＡＴ）を示すフローチャートである。

【図９５】

本発明の第７の実施形態における会員ＡＩＤの決定処理（MakeＰＡＴ）を示すフローチャートである。

【図９６】

本発明の第７の実施形態における会員ＡＩＤの決定処理（Merge ＰＡＴ）を示すフローチャートである。

【図９７】

本発明の第７の実施形態における会員ＡＩＤの決定処理（Split ＰＡＴ）を示すフローチャートである。

【図９８】

本発明の第７の実施形態における会員ＡＩＤの決定処理（Trans ＰＡＴ）を示すフローチャートである。

【図９９】

本発明の第７の実施形態におけるMerge ＰＡＴ命令を含むメッセージを示す図である。

【図１００】

本発明の第７の実施形態におけるSplit ＰＡＴ命令を含むメッセージを示す図である。

【図１０１】

本発明の第７の実施形態におけるTrans ＰＡＴ命令を含むメッセージを示す図である。

【符号の説明】

１　認証局ＣＡ

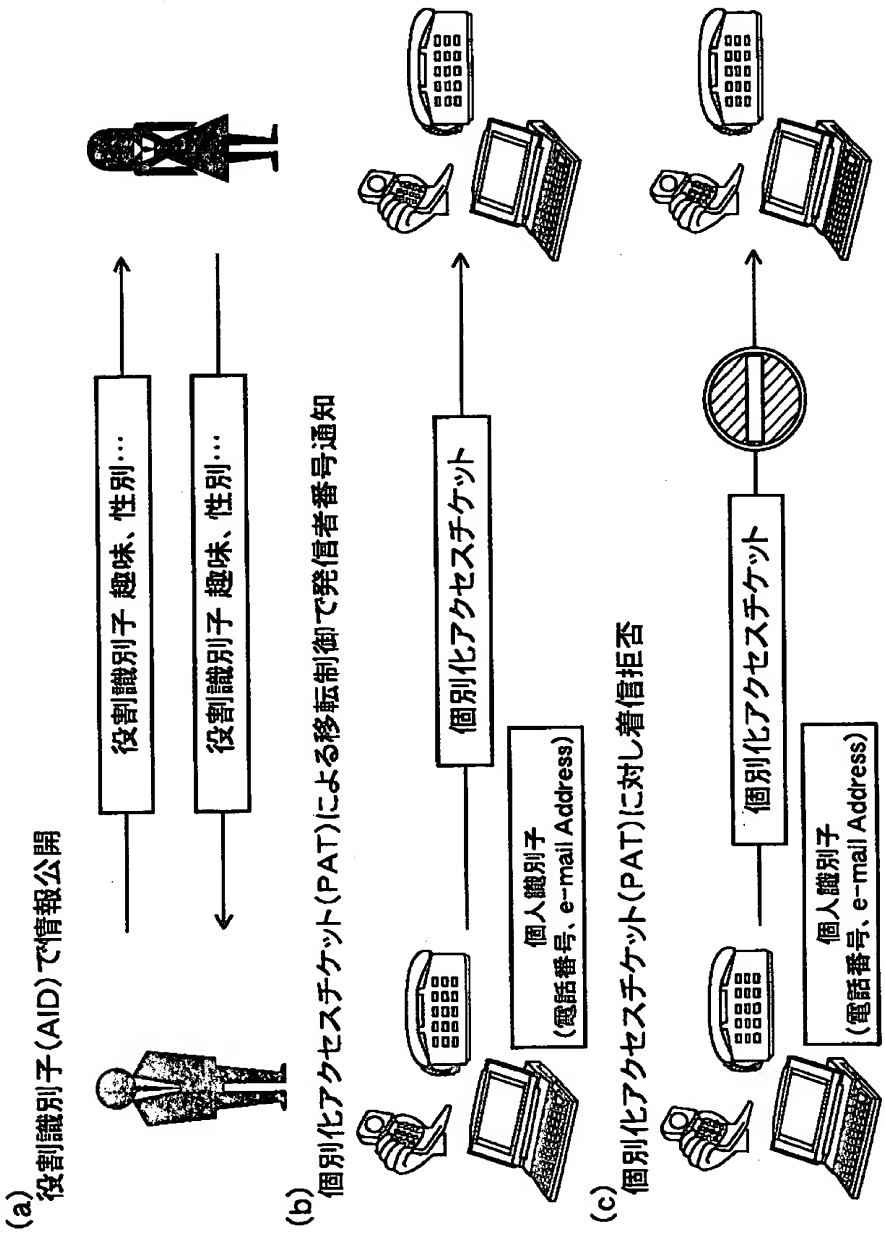
３　ユーザ

５　セキュア・コミュニケーション・サービスＳＣＳ

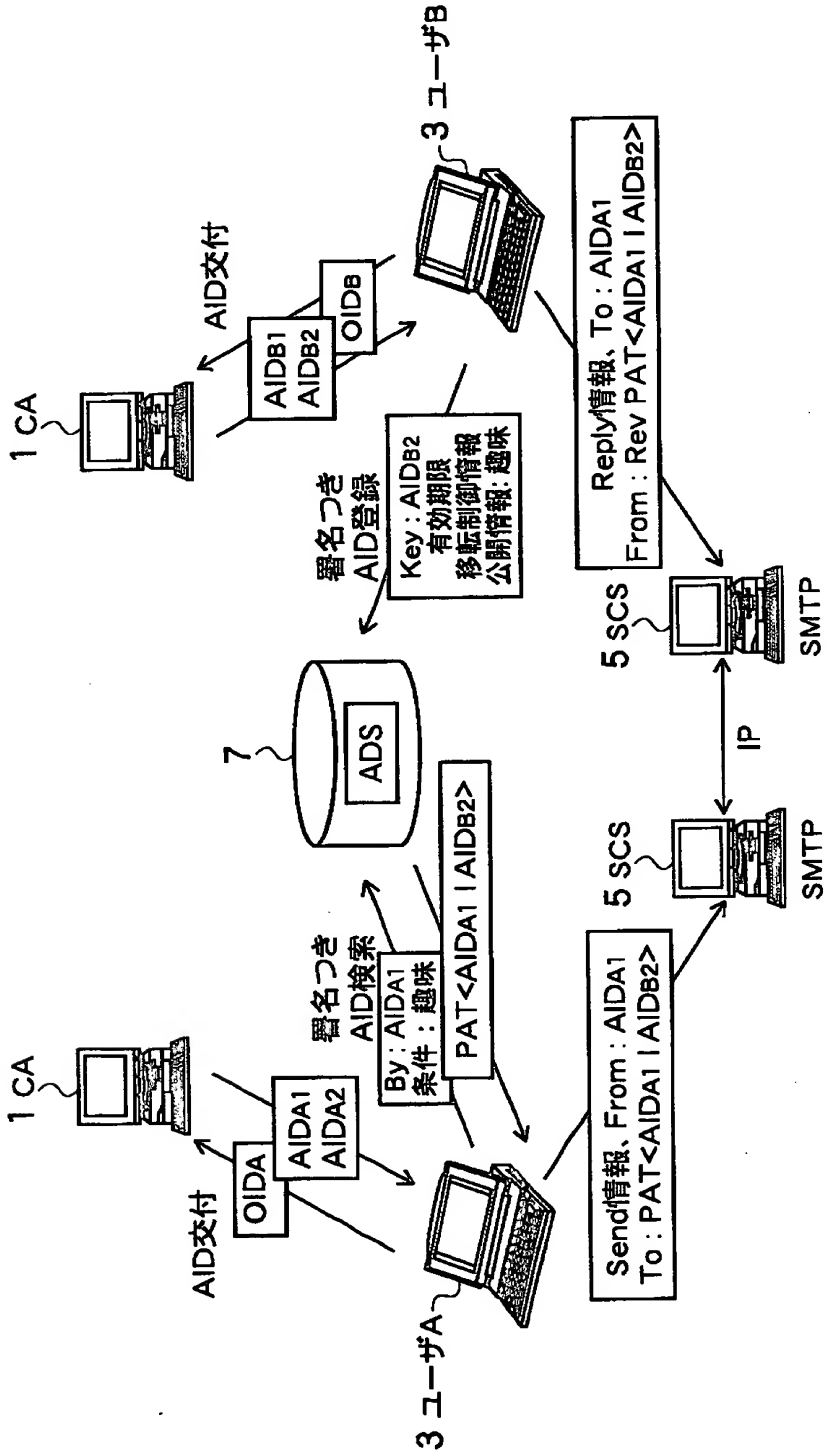
７　アノニマス・ディレクトリ・サービスＡＤＳ

【書類名】　　図面

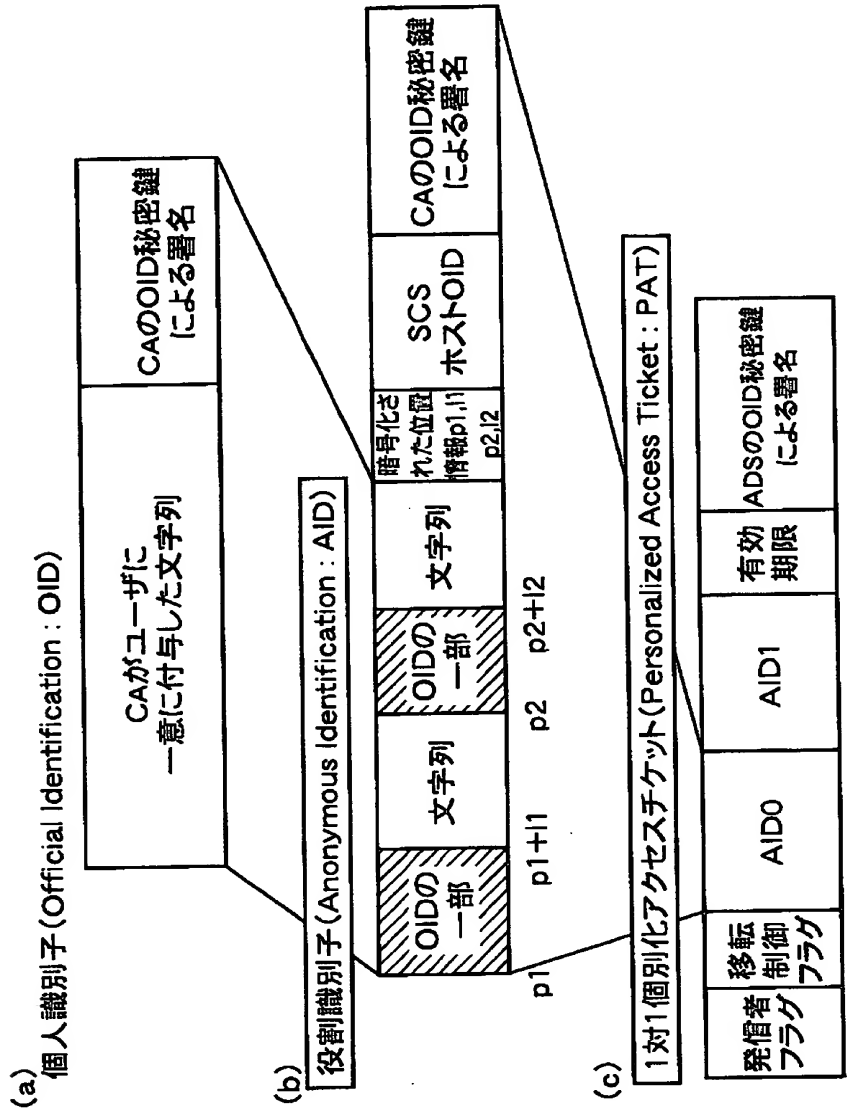
【図１】


(a)
役割識別子(AID)で情報公開
役割識別子 趣味、性別…
役割識別子 趣味、性別…
(b)
個別化アクセスチケット(PAT)による移転制御で発信者番号通知
個別化アクセスチケット
個人識別子
(電話番号、e-mail Address)
(c)
個別化アクセスチケット(PAT)に対し着信拒否
個別化アクセスチケット
個人識別子
(電話番号、e-mail Address)

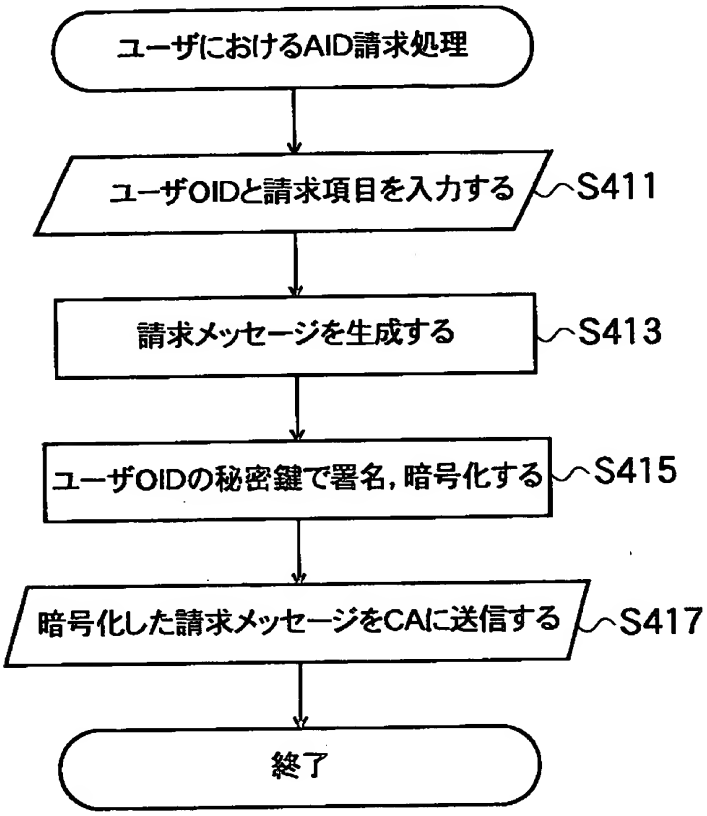
【図２】


1 CA
AID交付
AIDB1
AIDB2
OIDB
3 ユーザB
署名つき
AID登録
Key : AIDB2
有効期限
移転制御情報
公開情報 趣味
Reply情報、To : AIDA1
From : Rev PAT<AIDA1 | AIDB2>
5 SCS
SMTP
IP
7
ADS
署名つき
AID検索
By : AIDA1
条件 : 趣味
PAT<AIDA1 | AIDB2>
Send情報、From : AIDA1
To : PAT<AIDA1 | AIDB2>
1 CA
AID交付
OIDA
AIDA1
AIDA2
3 ユーザA

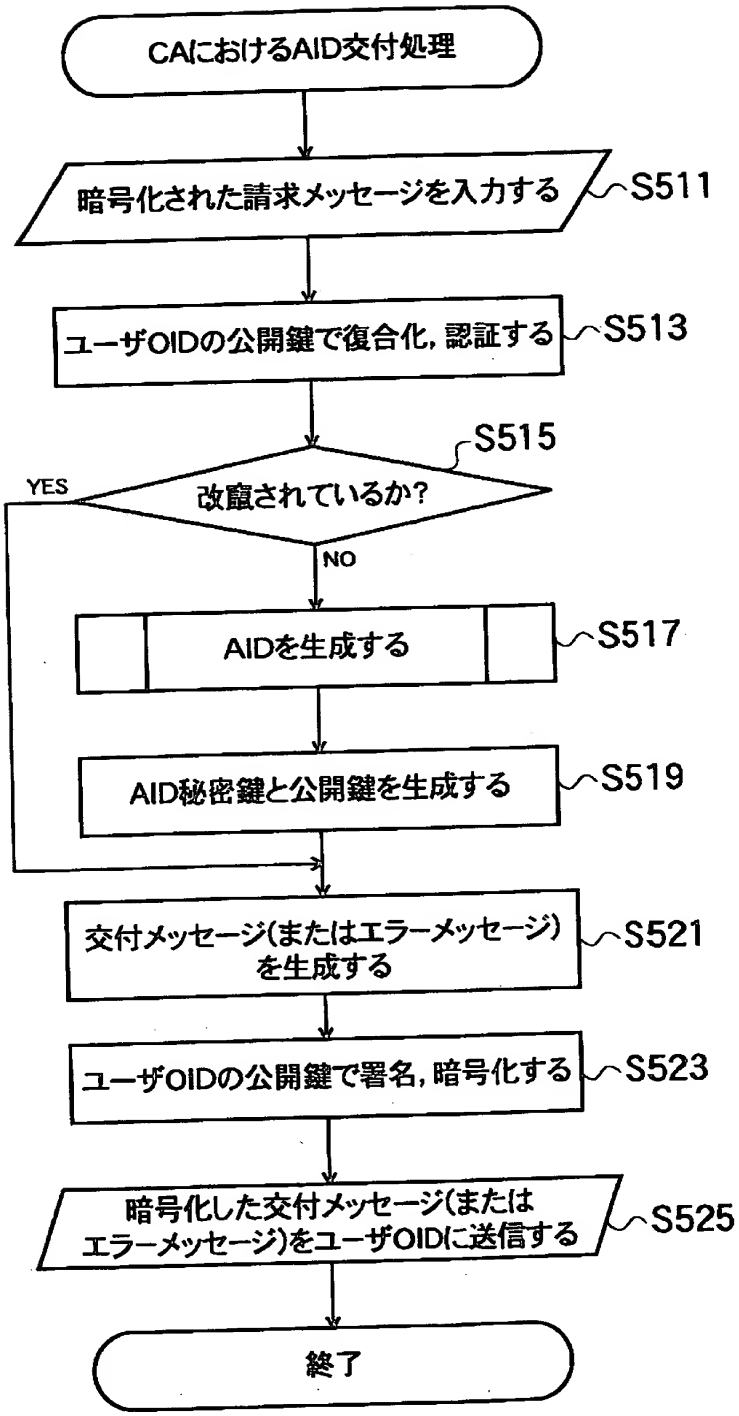
【図３】


(a)
個人識別子(Official Identification : OID)
CAがユーザに一意に付与した文字列
CAのOID秘密鍵による署名
(b)
役割識別子(Anonymous Identification : AID)
OIDの一部
文字列
OIDの一部
文字列
暗号化された位置情報p1,l1 p2,l2
SCS ホストOID
CAのOID秘密鍵による署名
p1
p1+l1
p2
p2+l2
(c)
1対1個別化アクセスチケット(Personalized Access Ticket : PAT)
発信者フラグ
移転制御フラグ
AID0
AID1
有効期限
ADSのOID秘密鍵による署名

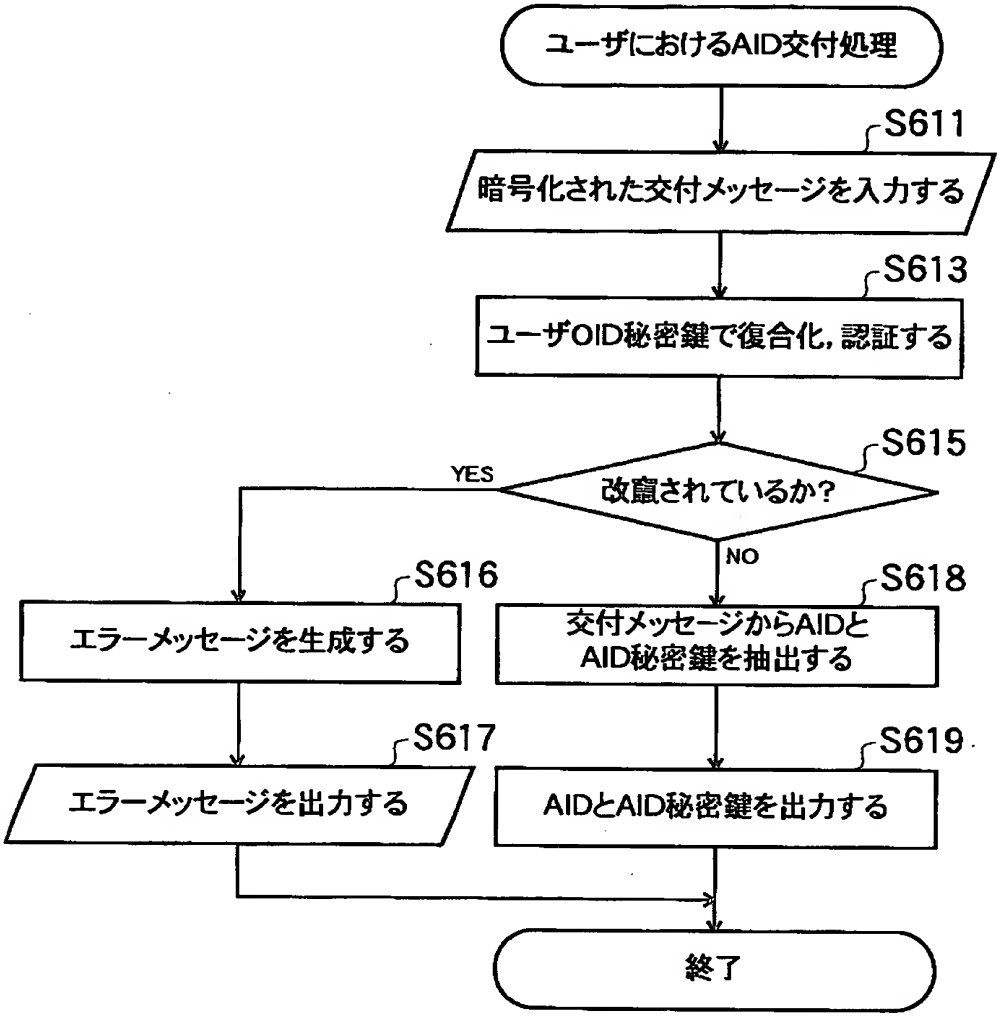
【図４】


ユーザにおけるAID請求処理
ユーザOIDと請求項目を入力する
S411
請求メッセージを生成する
S413
ユーザOIDの秘密鍵で署名，暗号化する
S415
暗号化した請求メッセージをCAに送信する
S417
終了

【図５】


CAにおけるAID交付処理
暗号化された請求メッセージを入力する
S511
ユーザOIDの公開鍵で復合化，認証する
S513
S515
改竄されているか?
YES
NO
AIDを生成する
S517
AID秘密鍵と公開鍵を生成する
S519
交付メッセージ(またはエラーメッセージ)を生成する
S521
ユーザOIDの公開鍵で署名，暗号化する
S523
暗号化した交付メッセージ(またはエラーメッセージ)をユーザOIDに送信する
S525
終了

【図６】


ユーザにおけるAID交付処理
S611
暗号化された交付メッセージを入力する
S613
ユーザOID秘密鍵で復合化，認証する
S615
改竄されているか?
YES
NO
S616
エラーメッセージを生成する
S618
交付メッセージからAIDと
AID秘密鍵を抽出する
S617
エラーメッセージを出力する
S619
AIDとAID秘密鍵を出力する
終了

【図７】

AID請求メッセージの例

REQUEST AID　2　　(新規AIDを2個請求する場合)

＜ユーザOIDの秘密鍵による署名＞
(送信時には，ユーザOIDの秘密鍵で暗号化する)

DISCARD AID AID1の実体　AID1の秘密鍵
DISCARD AID AID2の実体　AID2の秘密鍵
(既存AIDであるAID1とAID2を廃止したい場合)

＜ユーザOID秘密鍵による署名＞
(送信時には，ユーザOIDの秘密鍵で暗号化する)

【図８】

AID交付メッセージの例

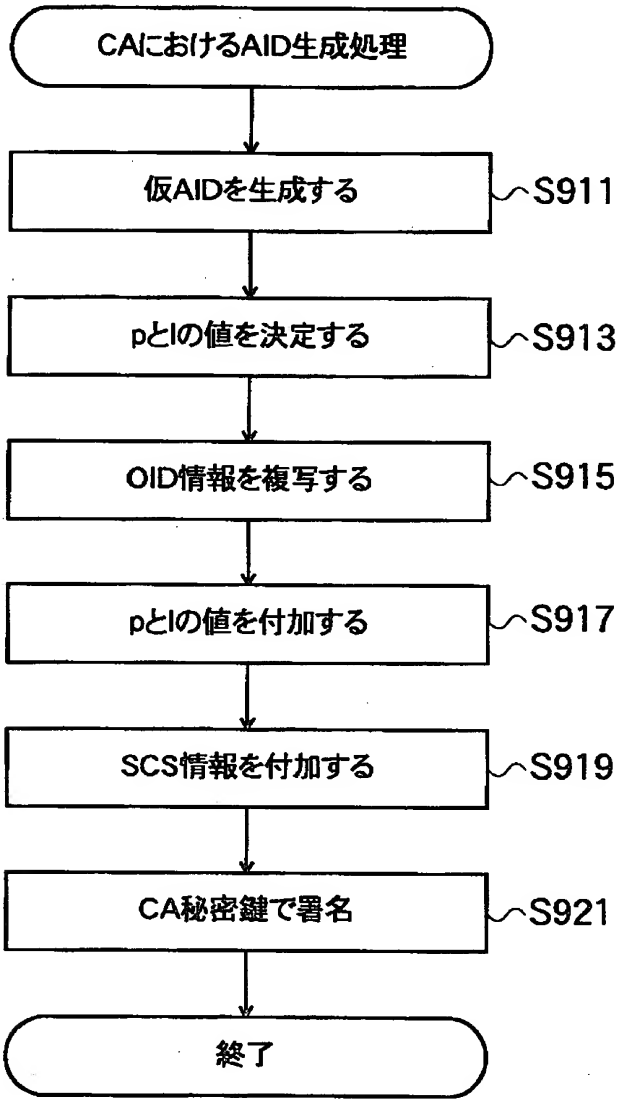
NEW AID AID3の実体　AID3の秘密鍵 OK
(新規AIDであるAID3は交付成功)
NEW AID NG　　(交付失敗,つまり,エラーメッセージ)

＜ユーザOIDの公開鍵による署名＞
(送信時には，ユーザOIDの公開鍵で暗号化する)

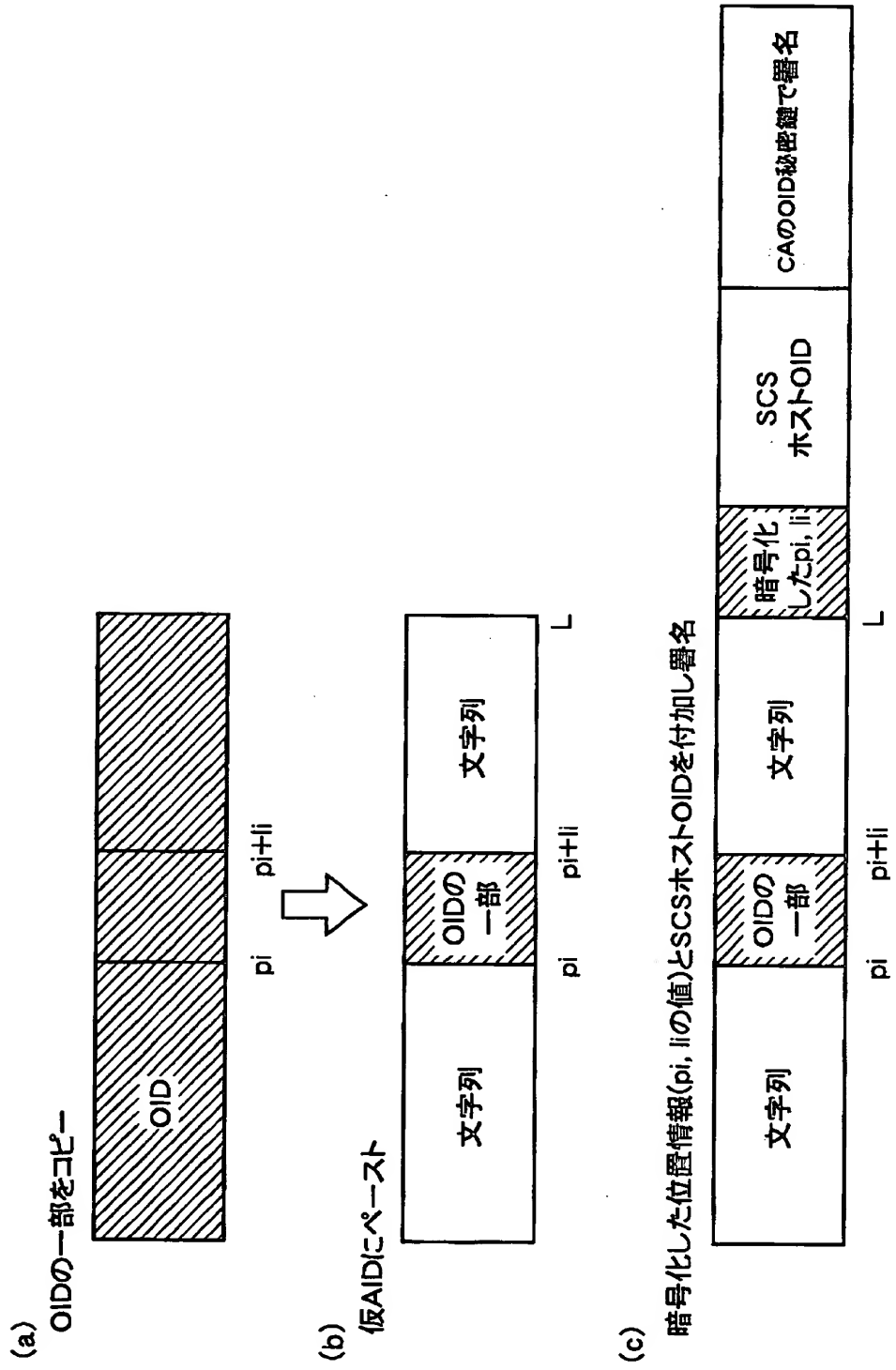
DISCARD AID AID1の実体 OK　　(既存AIDであるAID1は廃止成功)
DISCARD AID AID2の実体 NG
(既存AIDであるAID2の廃止失敗のエラーメッセージ)

＜ユーザOIDの公開鍵による署名＞
(送信時には，ユーザOIDの公開鍵で暗号化する)

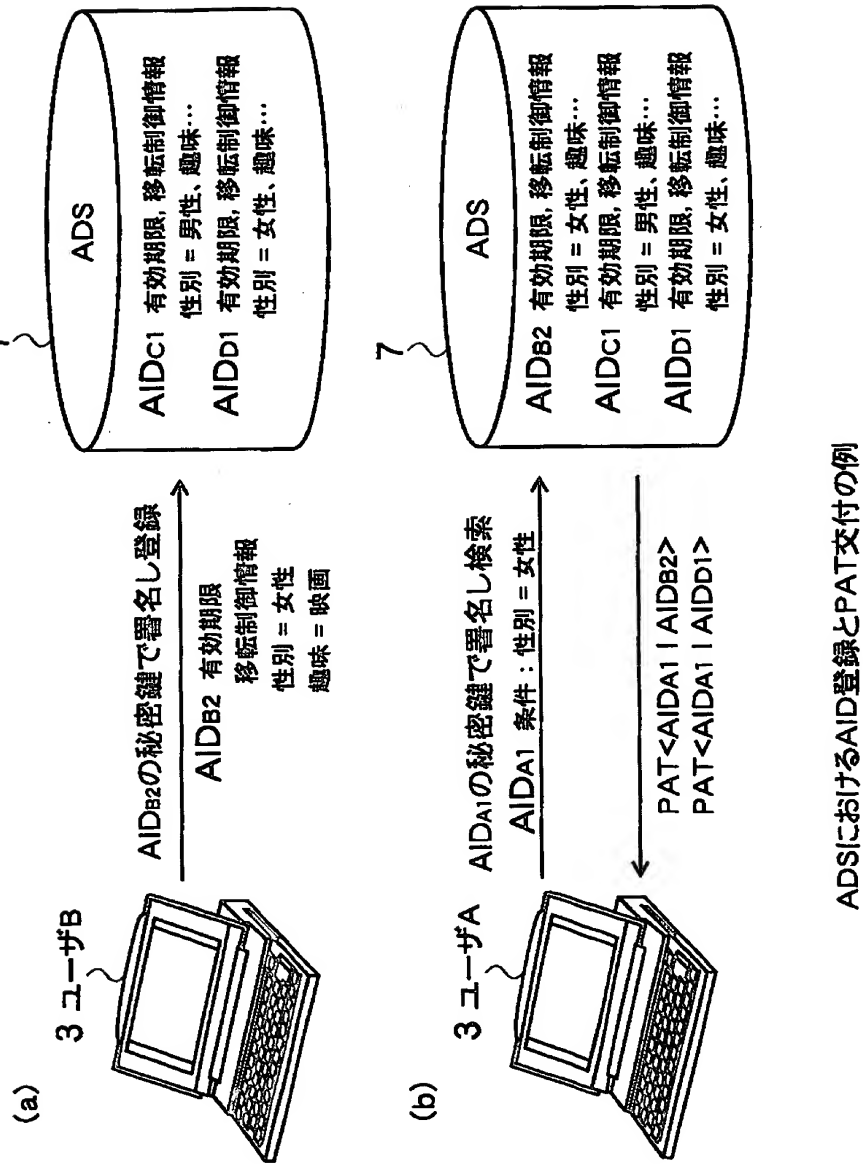
【図９】


CAにおけるAID生成処理
仮AIDを生成する
S911
pとlの値を決定する
S913
OID情報を複写する
S915
pとlの値を付加する
S917
SCS情報を付加する
S919
CA秘密鍵で署名
S921
終了

【図１０】

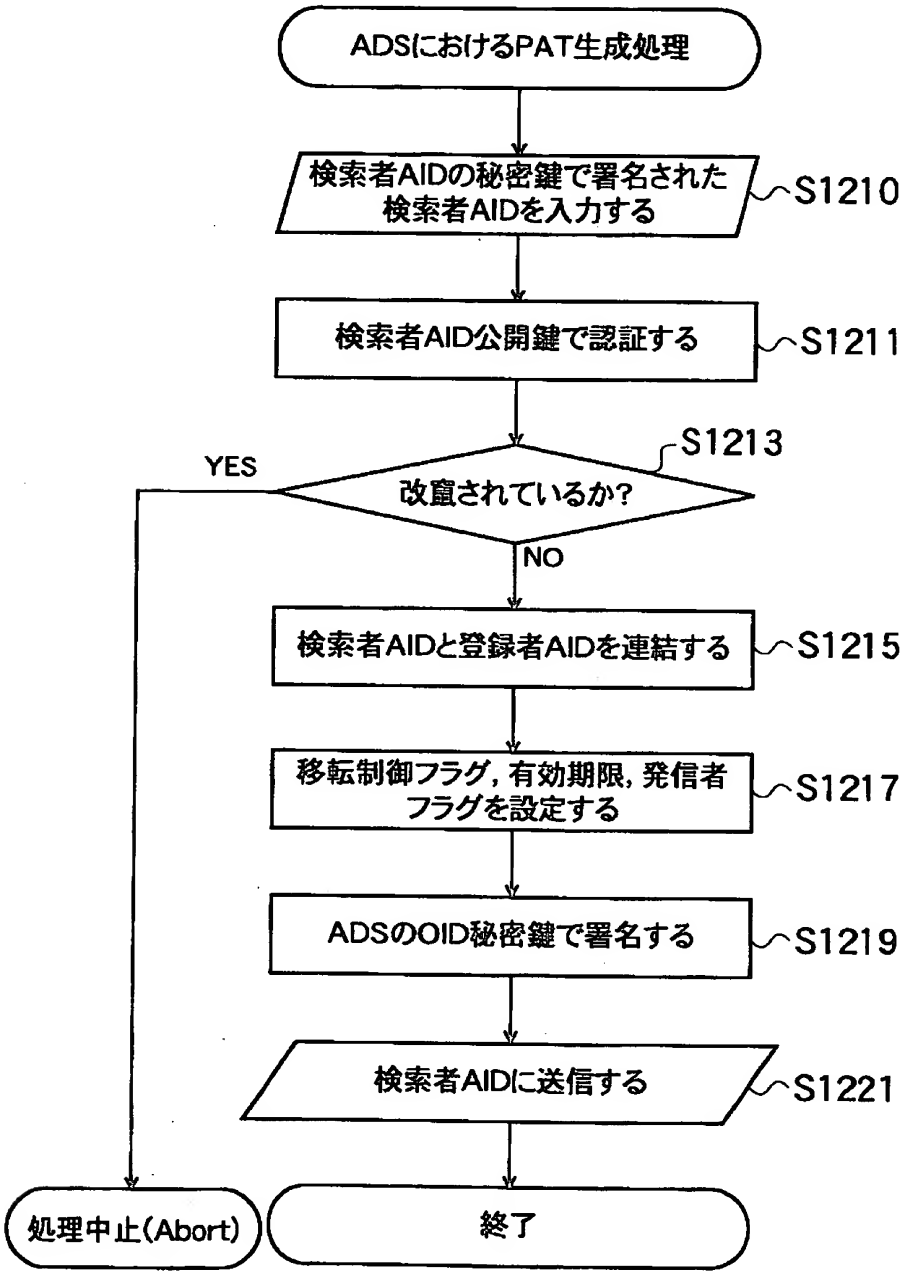

(a)
OIDの一部をコピー
OID
pi
pi+li
(b)
仮AIDにペースト
文字列
OIDの一部
文字列
pi
pi+li
L
(c)
暗号化した位置情報(pi, liの値)とSCSホストOIDを付加し署名
文字列
OIDの一部
文字列
暗号化したpi, li
SCSホストOID
CAのOID秘密鍵で署名
pi
pi+li
L

【図１１】

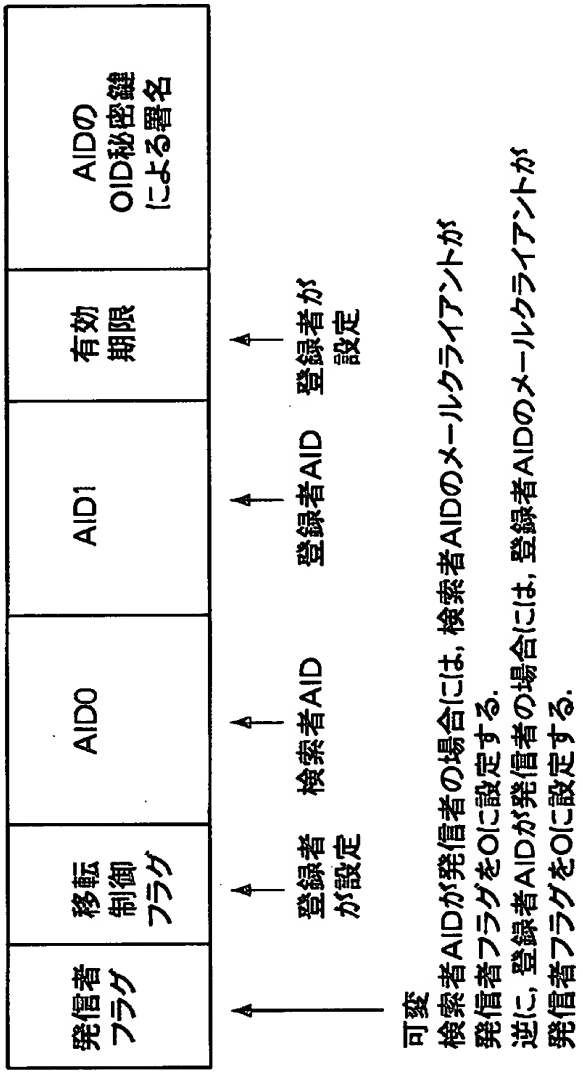


ADSにおけるAID登録とPAT交付の例

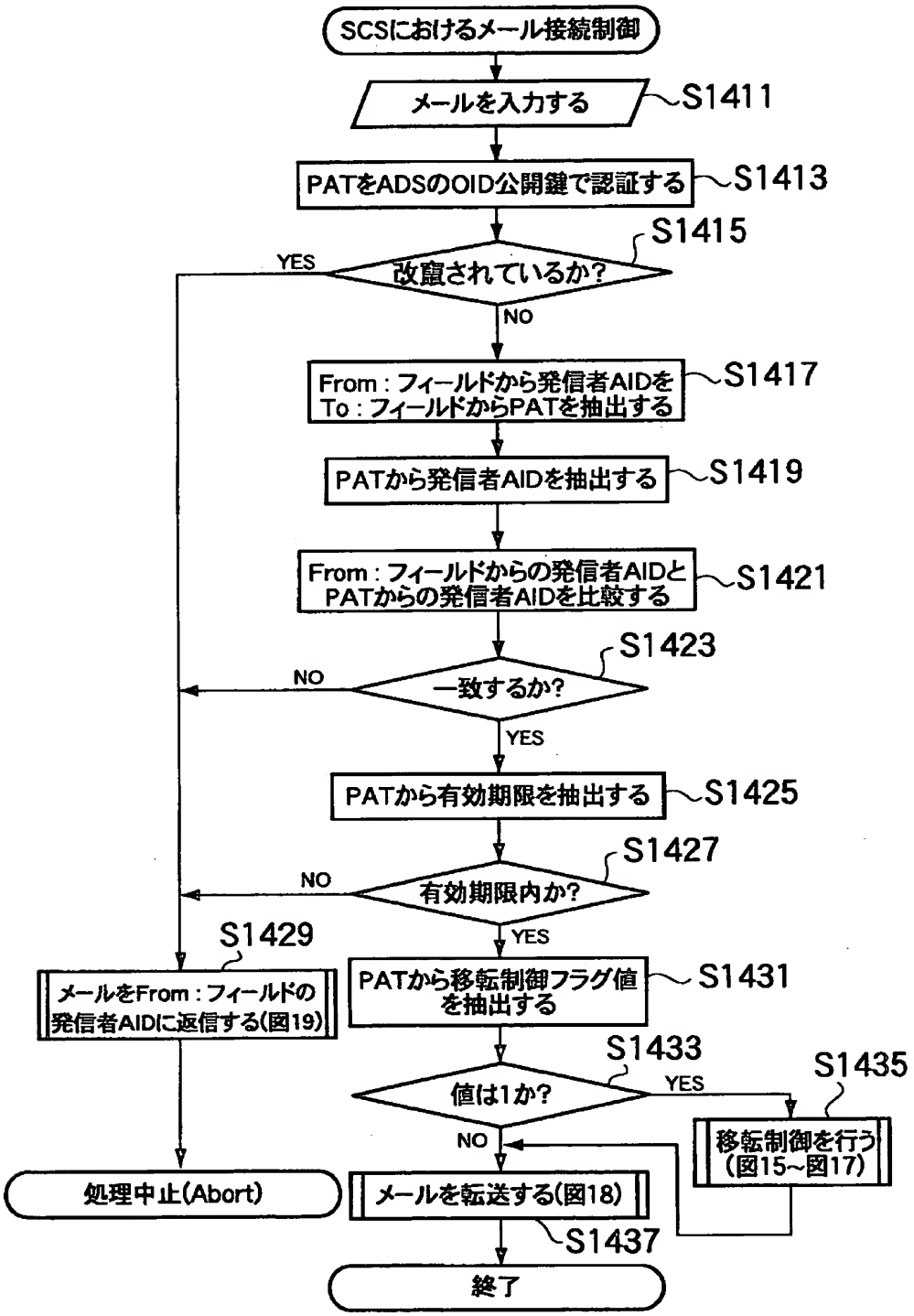
【図１２】


ADSにおけるPAT生成処理
検索者AIDの秘密鍵で署名された検索者AIDを入力する
S1210
検索者AID公開鍵で認証する
S1211
S1213
YES
改竄されているか?
NO
検索者AIDと登録者AIDを連結する
S1215
移転制御フラグ，有効期限，発信者フラグを設定する
S1217
ADSのOID秘密鍵で署名する
S1219
検索者AIDに送信する
S1221
処理中止(Abort)
終了

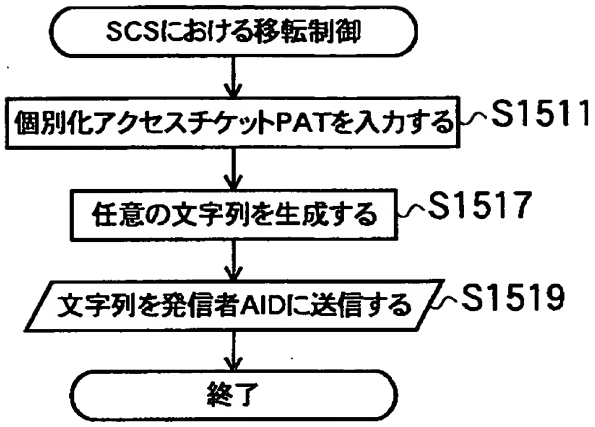
【図１３】


発信者フラグ
移転制御フラグ
AID0
AID1
有効期限
AIDのOID秘密鍵による署名
登録者が設定
検索者AID
登録者AID
登録者が設定
可変
検索者AIDが発信者の場合には，検索者AIDのメールクライアントが
発信者フラグをOに設定する．
逆に，登録者AIDが発信者の場合には，登録者AIDのメールクライアントが
発信者フラグをOに設定する．

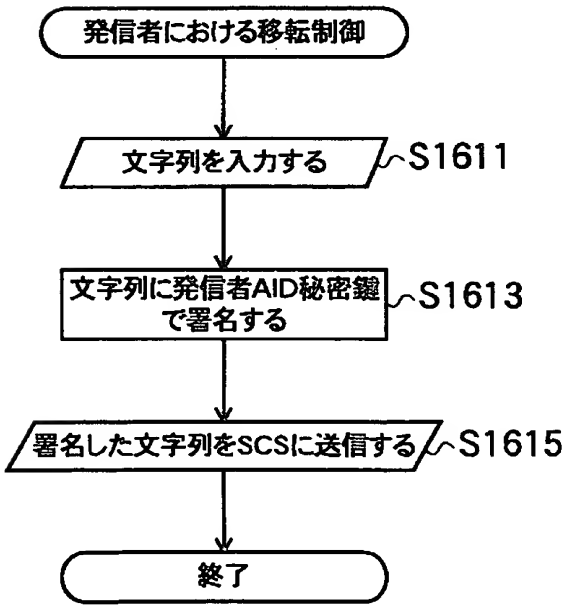
【図１４】


SCSにおけるメール接続制御
メールを入力する
S1411
PATをADSのOID公開鍵で認証する
S1413
S1415
改竄されているか?
YES
NO
From : フィールドから発信者AIDを
To : フィールドからPATを抽出する
S1417
PATから発信者AIDを抽出する
S1419
From : フィールドからの発信者AIDと
PATからの発信者AIDを比較する
S1421
S1423
一致するか?
NO
YES
PATから有効期限を抽出する
S1425
S1427
有効期限内か?
NO
YES
S1429
メールをFrom : フィールドの
発信者AIDに返信する(図19)
PATから移転制御フラグ値
を抽出する
S1431
S1433
値は1か?
YES
S1435
移転制御を行う
(図15~図17)
NO
処理中止(Abort)
メールを転送する(図18)
S1437
終了

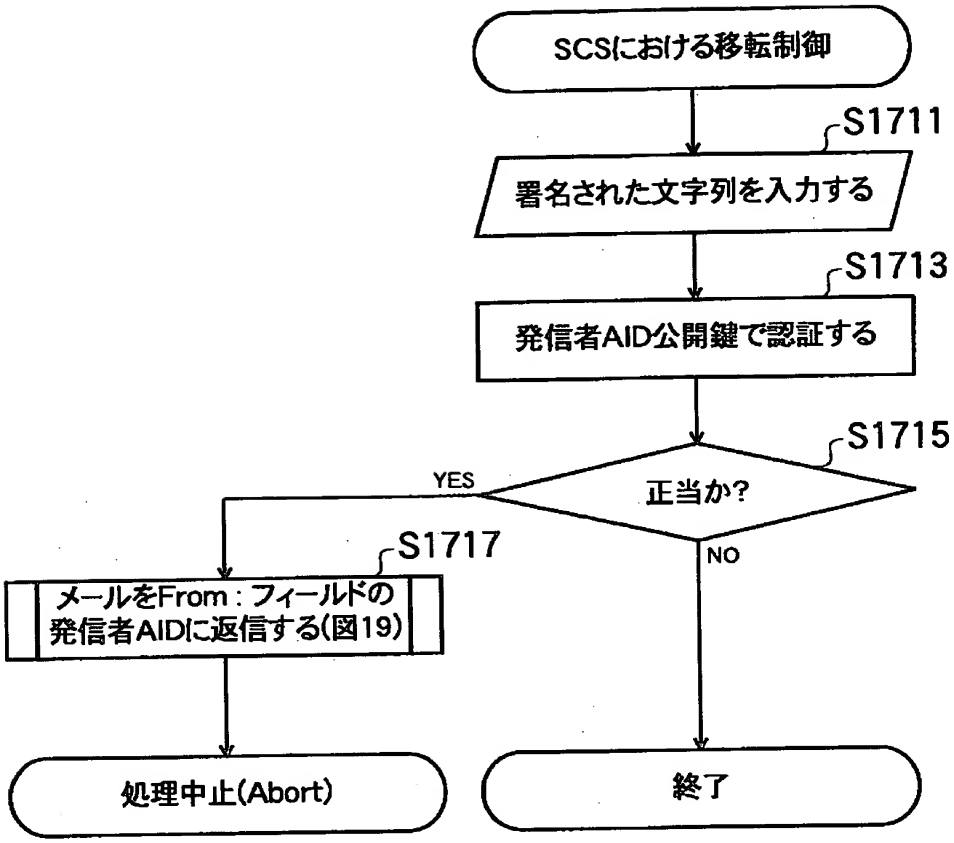
【図１５】


SCSにおける移転制御
個別化アクセスチケットPATを入力する
S1511
任意の文字列を生成する
S1517
文字列を発信者AIDに送信する
S1519
終了

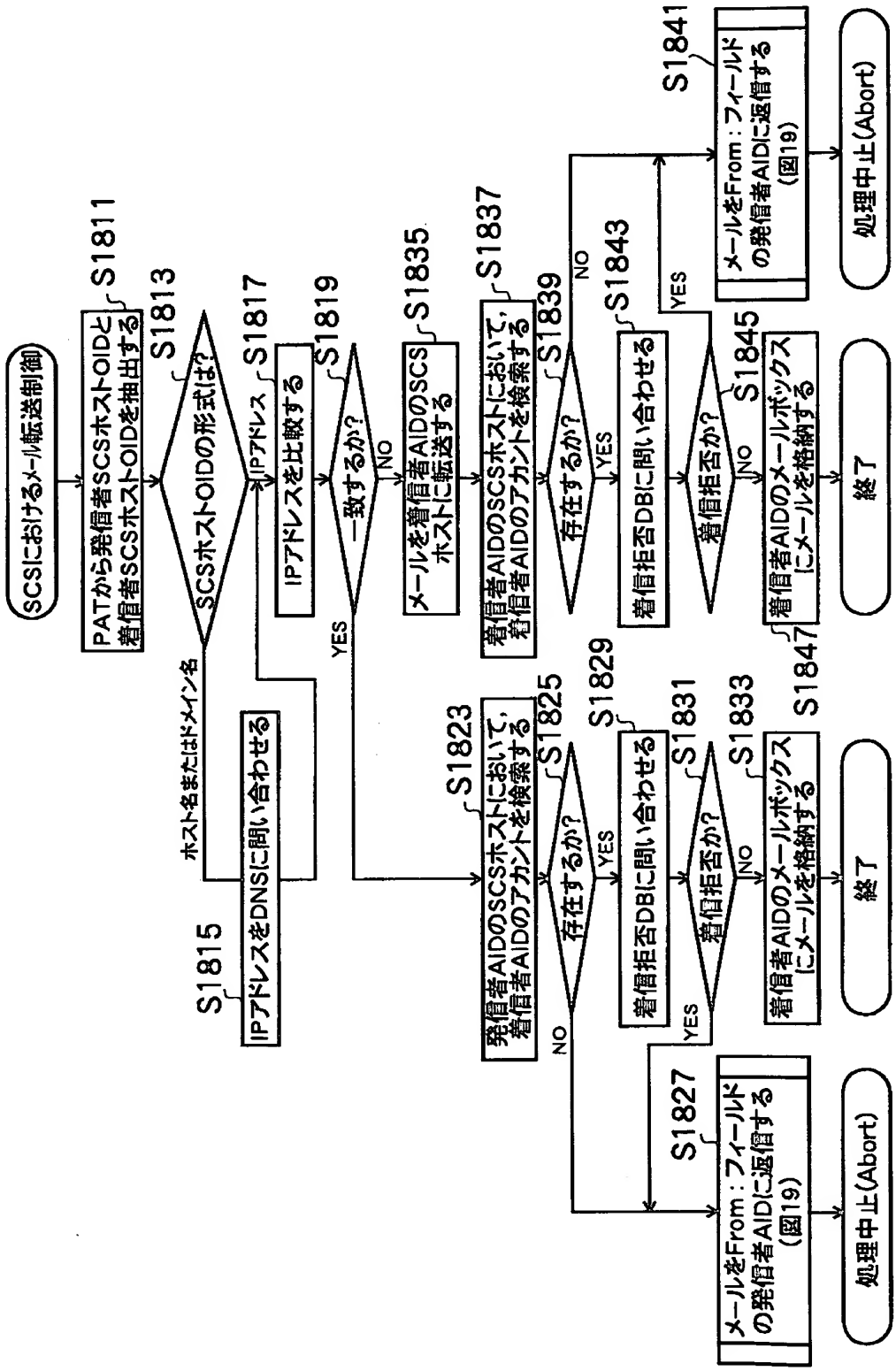
【図１６】


発信者における移転制御
文字列を入力する
S1611
文字列に発信者AID秘密鍵で署名する
S1613
署名した文字列をSCSに送信する
S1615
終了

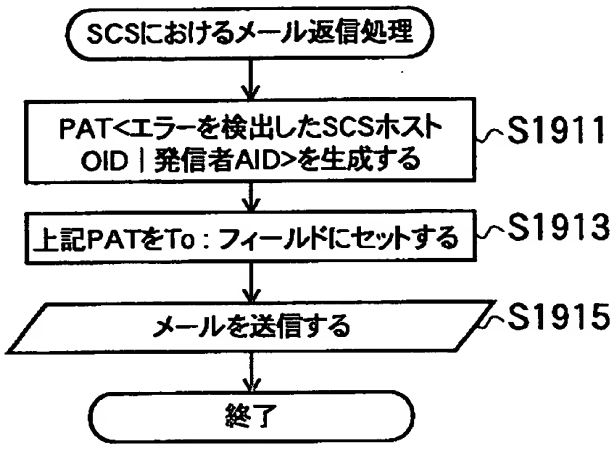
【図１７】


SCSにおける移転制御
S1711
署名された文字列を入力する
S1713
発信者AID公開鍵で認証する
S1715
正当か?
YES
NO
S1717
メールをFrom：フィールドの
発信者AIDに返信する(図19)
処理中止(Abort)
終了

【図１８】


SCSにおけるメール転送制御
S1811
PATから発信者SCSホストOIDと着信者SCSホストOIDを抽出する
S1813
SCSホストOIDの形式は?
ホスト名またはドメイン名
S1815
IPアドレスをDNSに問い合わせる
IPアドレス
S1817
IPアドレスを比較する
S1819
一致するか?
YES
NO
S1823
発信者AIDのSCSホストにおいて,着信者AIDのアカントを検索する
S1825
存在するか?
NO
YES
S1827
メールをFrom:フィールドの発信者AIDに返信する(図19)
処理中止(Abort)
S1829
着信拒否DBに問い合わせる
S1831
着信拒否か?
YES
NO
S1833
着信者AIDのメールボックスにメールを格納する
S1847
終了
S1835
メールを着信者AIDのSCSホストに転送する
S1837
着信者AIDのSCSホストにおいて,着信者AIDのアカントを検索する
S1839
存在するか?
NO
YES
S1841
メールをFrom:フィールドの発信者AIDに返信する(図19)
処理中止(Abort)
S1843
着信拒否DBに問い合わせる
S1845
着信拒否か?
YES
NO
着信者AIDのメールボックスにメールを格納する
終了

【図１９】



【図２０】

クライアント間の電子メールの例

送信

From : <ユーザAのAID>
To : PAT<ユーザAのAID | ユーザBのAID>
Subject : こんにちわ

いい天気ですね.

返信

From : <ユーザBのAID>
To : Rev PAT<ユーザAのAID | ユーザBのAID>
Subject : Re : こんにちわ

そうですね.

PAT<A | B>は発信者フラグが0(つまり発信者はA)のPAT
Rev PAT<A | B>は発信者フラグが1(つまり発信者はB)のPAT

【図２１】

着信拒否された場合の電子メールの例

送信

From : <ユーザAのAID>
To : PAT<ユーザAのAID | ユーザBのAID>
Subject : こんにちわ

いい天気ですね.

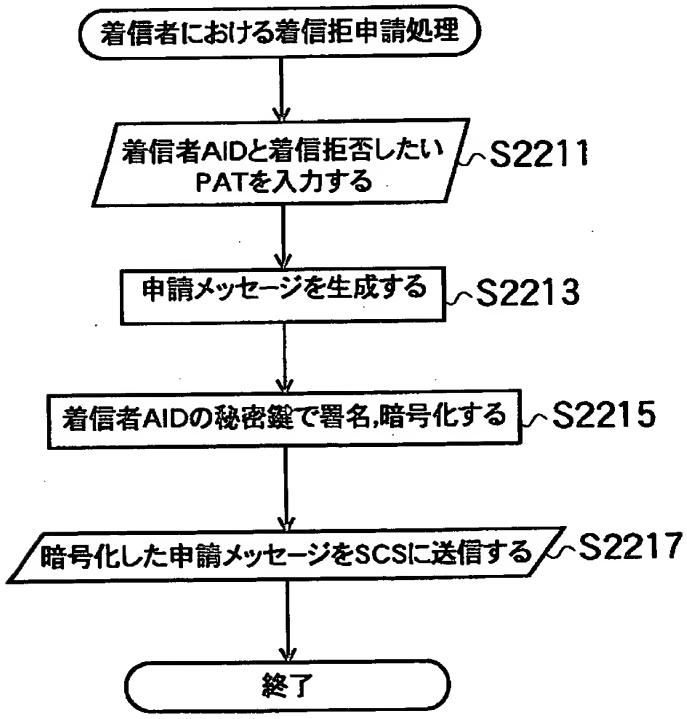
返信

From : <SCSのホストOID>
To : PAT<SCSのホストOID | ユーザAのAID>
Subject : 着信拒否通知

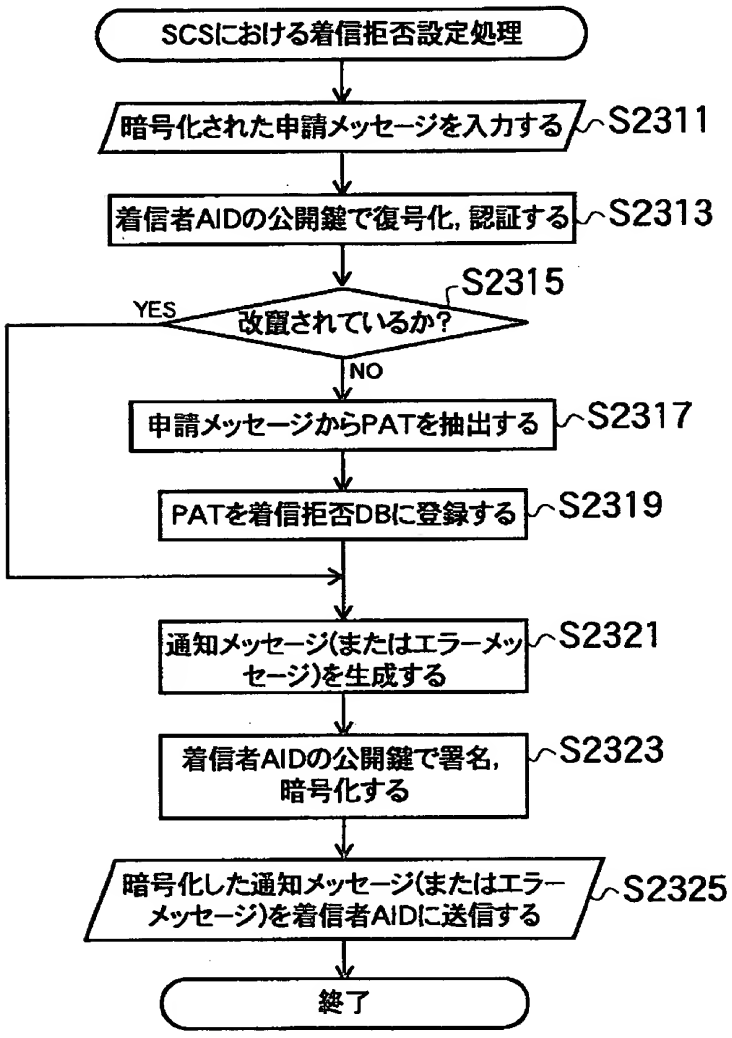
以下のメールは着信拒否されています.

>From : <ユーザAのAID>
>To : PAT<ユーザAのAID | ユーザBのAID>
>Subject : こんにちわ
>
>いい天気ですね.

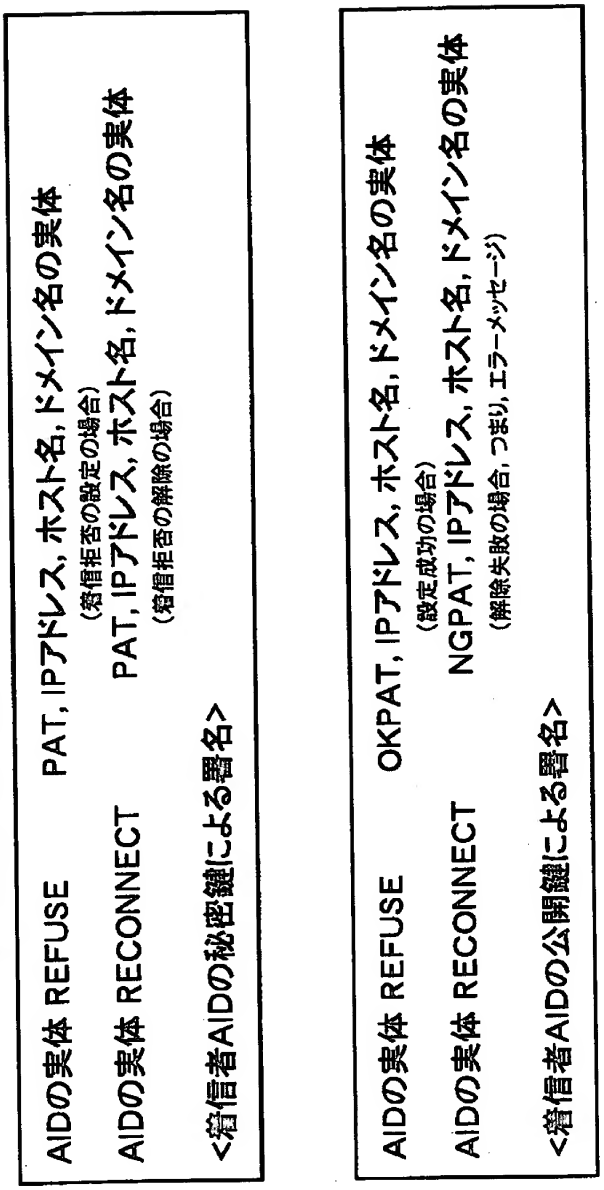
【図２２】



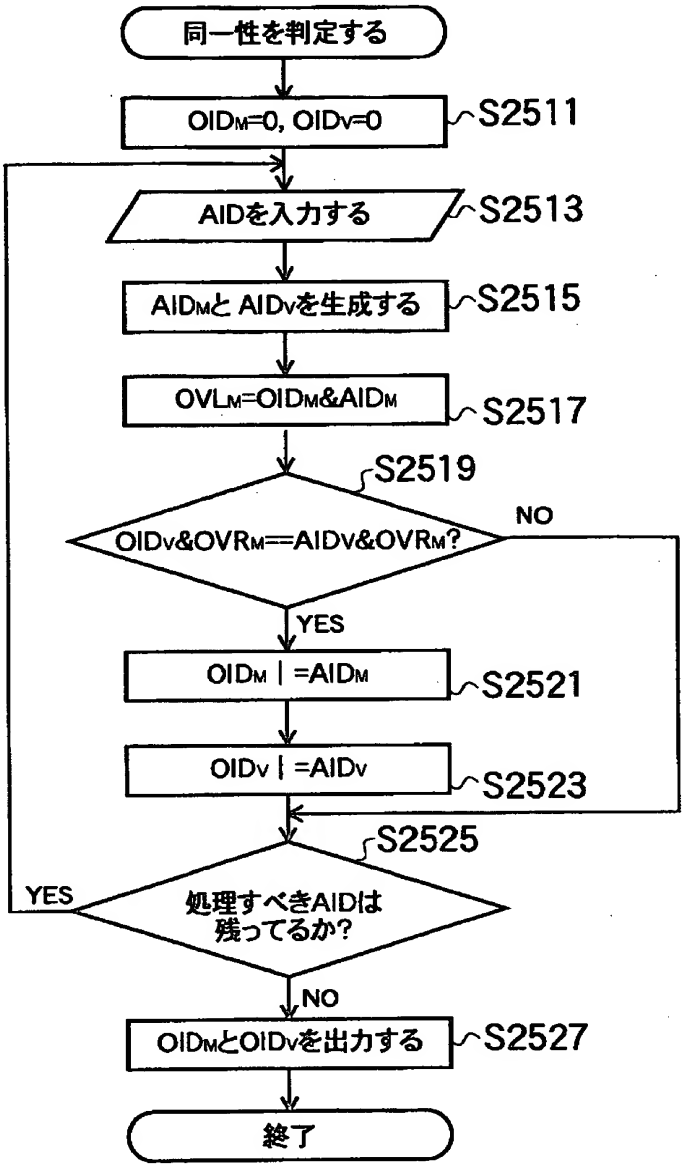
【図２３】


SCSにおける着信拒否設定処理
暗号化された申請メッセージを入力する
S2311
着信者AIDの公開鍵で復号化，認証する
S2313
S2315
YES
改竄されているか？
NO
申請メッセージからPATを抽出する
S2317
PATを着信拒否DBに登録する
S2319
通知メッセージ(またはエラーメッセージ)を生成する
S2321
着信者AIDの公開鍵で署名，暗号化する
S2323
暗号化した通知メッセージ(またはエラーメッセージ)を着信者AIDに送信する
S2325
終了

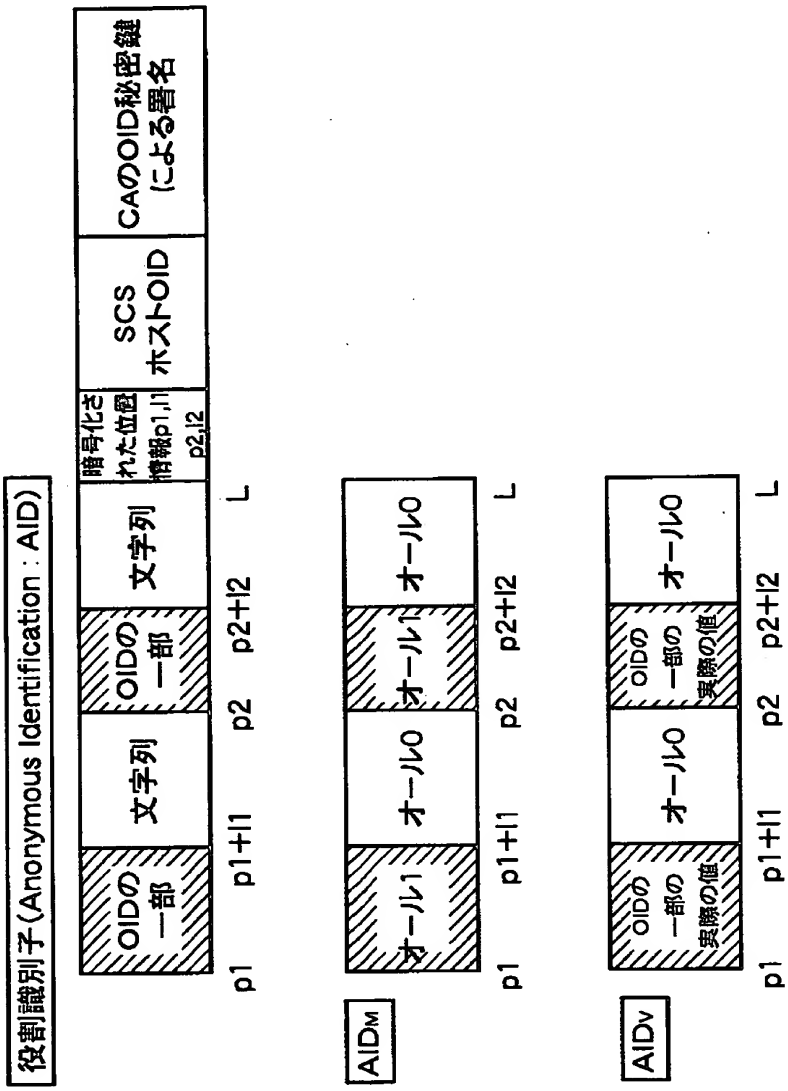
【図２４】


着信拒否申請・通知メッセージの例
AIDの実体 REFUSE PAT, IPアドレス, ホスト名, ドメイン名の実体
(着信拒否の設定の場合)
AIDの実体 RECONNECT PAT, IPアドレス, ホスト名, ドメイン名の実体
(着信拒否の解除の場合)
<着信者AIDの秘密鍵による署名>
AIDの実体 REFUSE OKPAT, IPアドレス, ホスト名, ドメイン名の実体
(設定成功の場合)
AIDの実体 RECONNECT NGPAT, IPアドレス, ホスト名, ドメイン名の実体
(解除失敗の場合, つまり, エラーメッセージ)
<着信者AIDの公開鍵による署名>

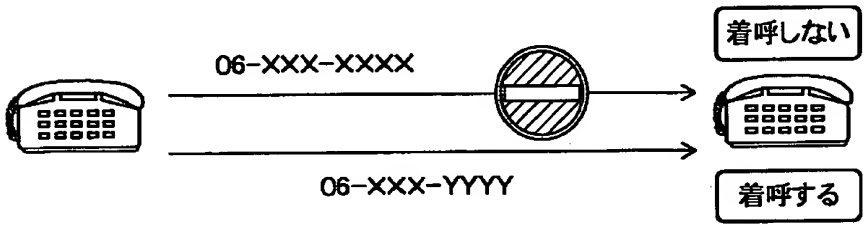
【図２５】


同一性を判定する
OIDM=0, OIDV=0
S2511
AIDを入力する
S2513
AIDMと AIDVを生成する
S2515
OVLM=OIDM&AIDM
S2517
S2519
OIDV&OVRM==AIDV&OVRM?
NO
YES
OIDM | =AIDM
S2521
OIDV | =AIDV
S2523
S2525
YES
処理すべきAIDは
残ってるか?
NO
OIDMとOIDVを出力する
S2527
終了

【図２６】

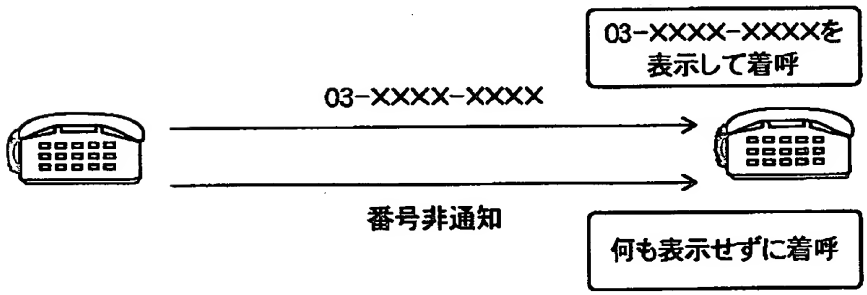

役割識別子(Anonymous Identification : AID)
OIDの一部
文字列
OIDの一部
文字列
暗号化された位置情報p1,l1 p2,l2
SCSホストOID
CAのOID秘密鍵による署名
p1
p1+l1
p2
p2+l2
L
AIDM
オール1
オール0
オール1
オール0
AIDV
OIDの一部 実際の値
オール0
OIDの一部 実際の値
オール0

【図２７】



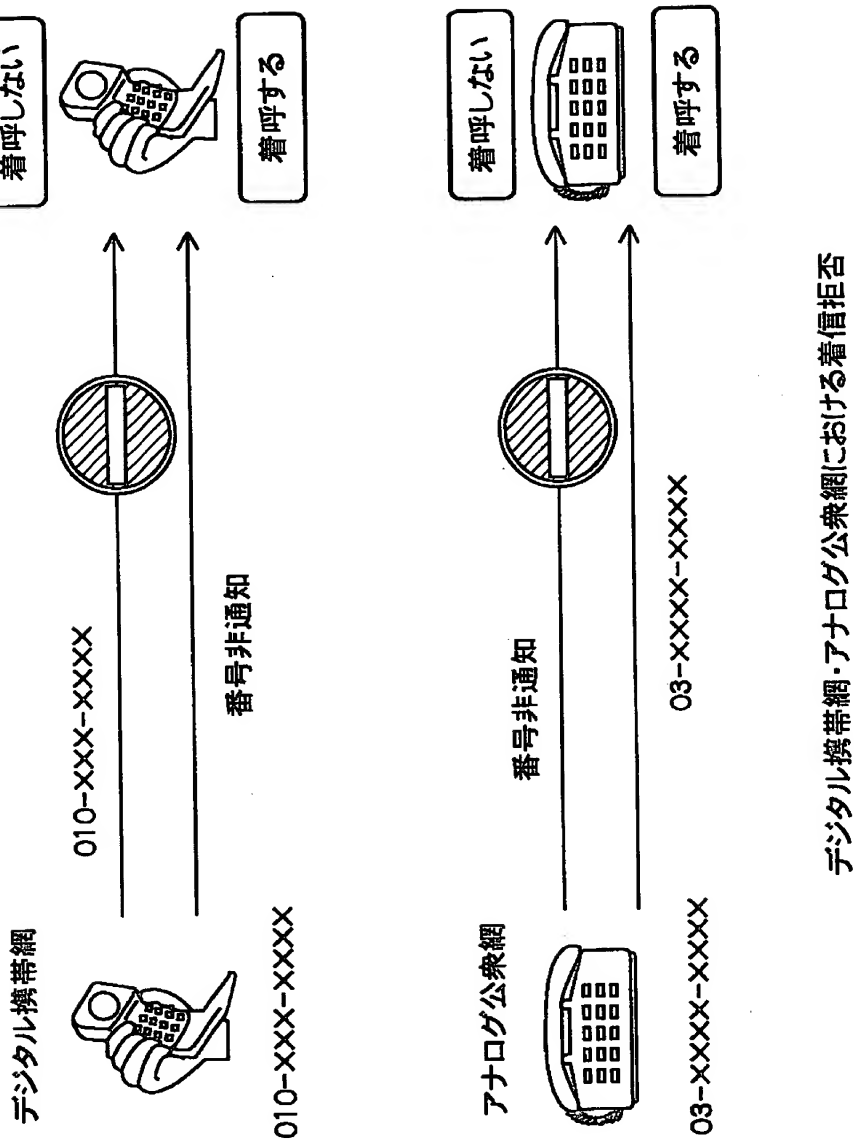
アナログ公衆網における二重番号登録

【図２８】



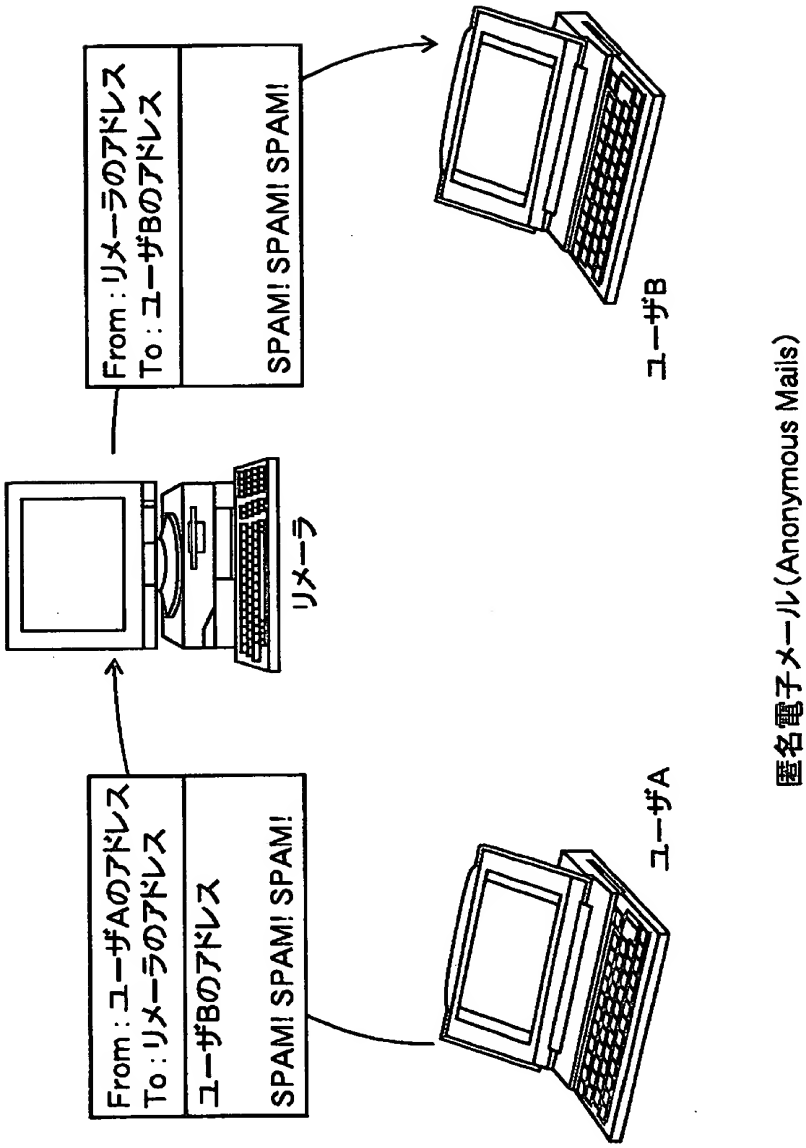
アナログ公衆網における発信者番号通知

【図２９】

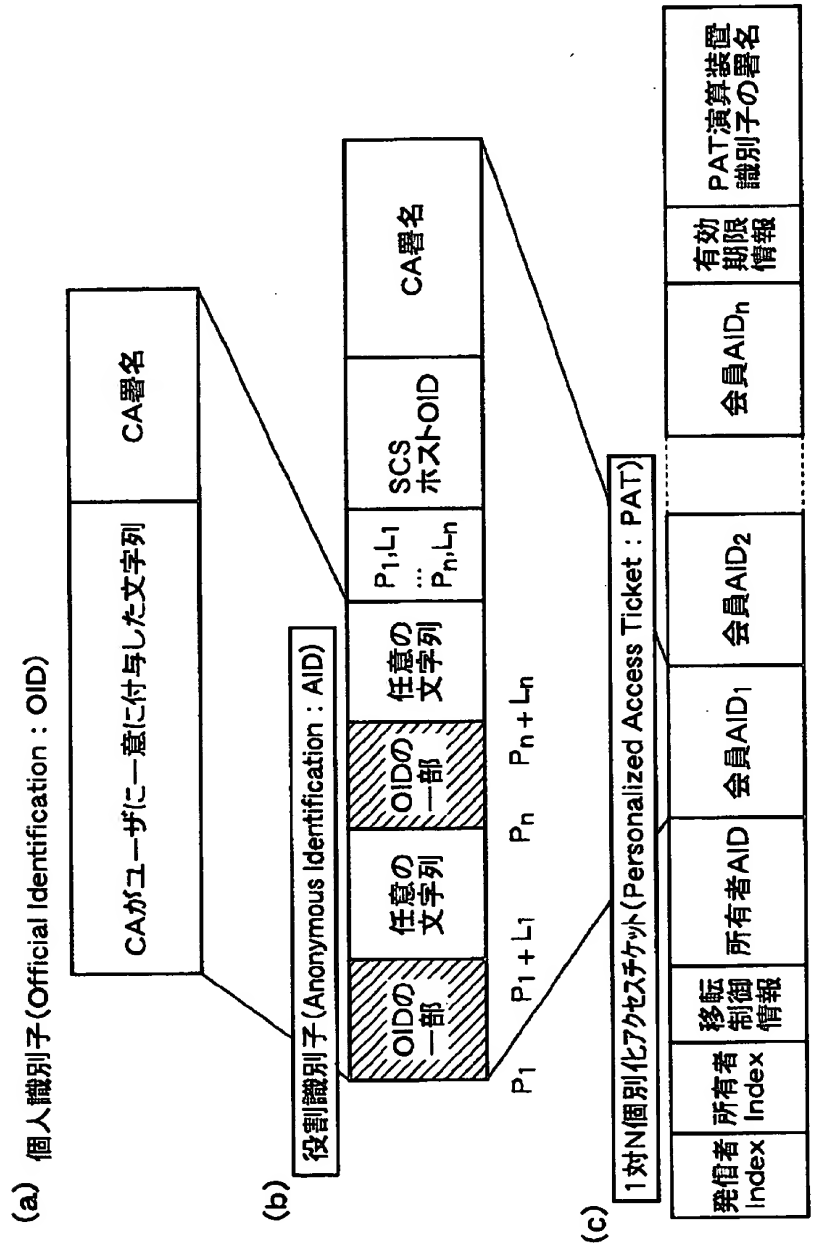


デジタル携帯網・アナログ公衆網における着信拒否

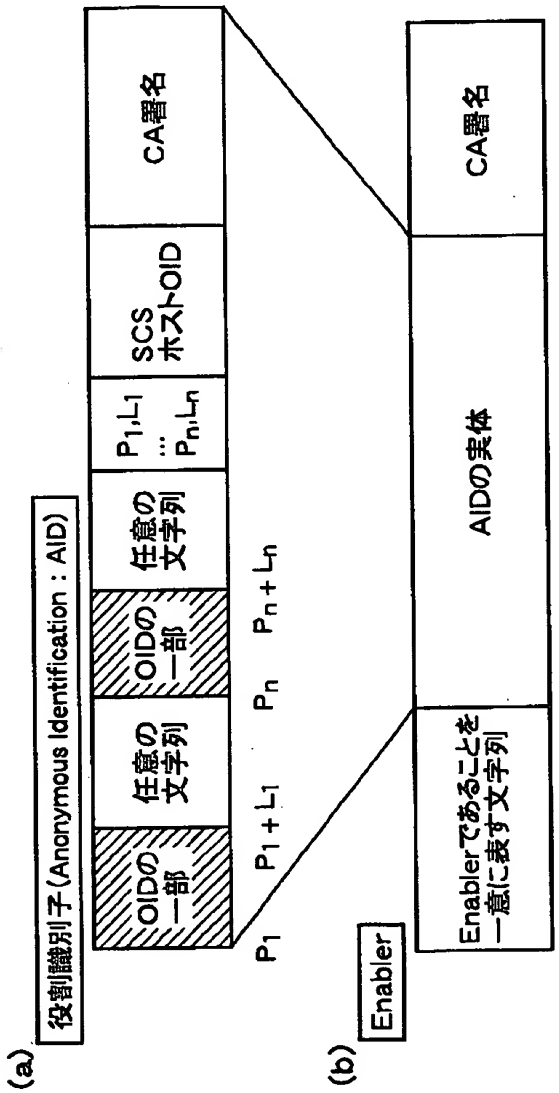
【図３０】


From：リメーラのアドレス
To：ユーザBのアドレス
SPAM! SPAM! SPAM!
ユーザB
リメーラ
From：ユーザAのアドレス
To：リメーラのアドレス
ユーザBのアドレス
SPAM! SPAM! SPAM!
ユーザA
匿名電子メール(Anonymous Mails)

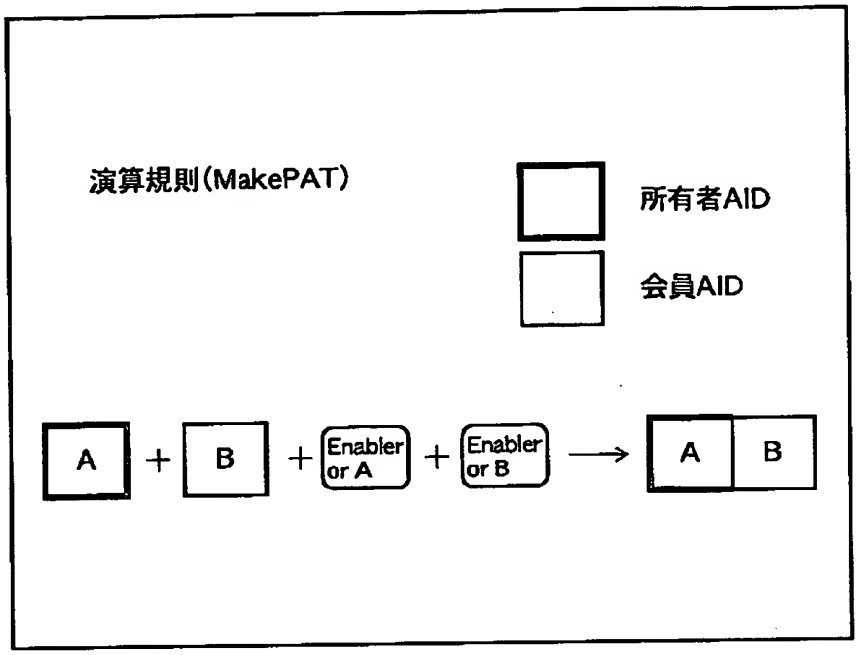
【図３１】


(a) 個人識別子(Official Identification : OID)
CAがユーザに一意に付与した文字列
CA署名
(b)
役割識別子(Anonymous Identification : AID)
OIDの一部
任意の文字列
OIDの一部
任意の文字列
P1,L1 … Pn,Ln
SCS ホストOID
CA署名
P1
P1 + L1
Pn
Pn + Ln
(c)
1対N個別化アクセスチケット(Personalized Access Ticket : PAT)
発信者 Index
所有者 Index
移転制御情報
所有者AID
会員AID1
会員AID2
会員AIDn
有効期限情報
PAT演算装置識別子の署名

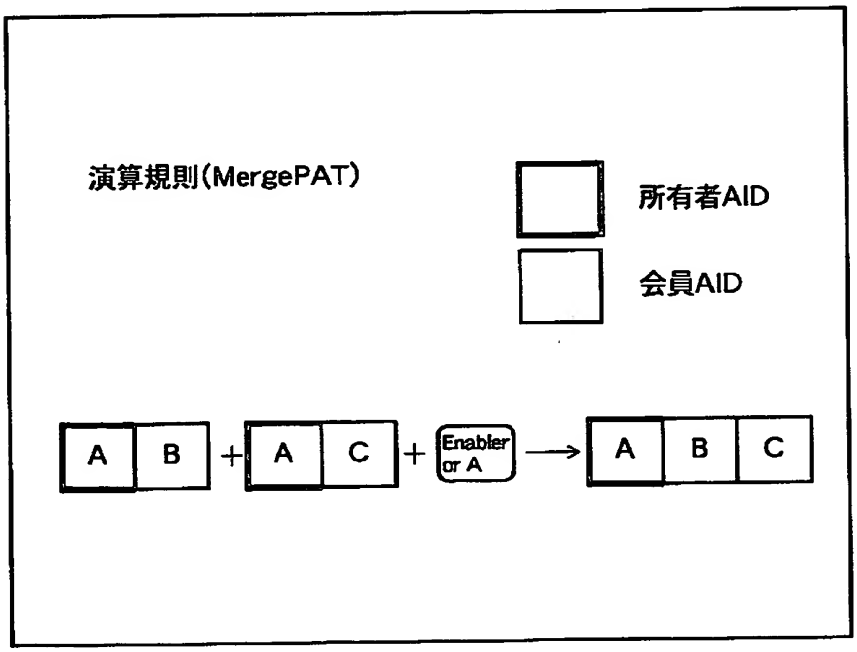
【図３２】


(a)
役割識別子(Anonymous Identification : AID)
OIDの一部
任意の文字列
OIDの一部
任意の文字列
P1,L1
...
Pn,Ln
SCSホストOID
CA署名
P1
P1+L1
Pn
Pn+Ln
(b)
Enabler
Enablerであることを一意に表す文字列
AIDの実体
CA署名

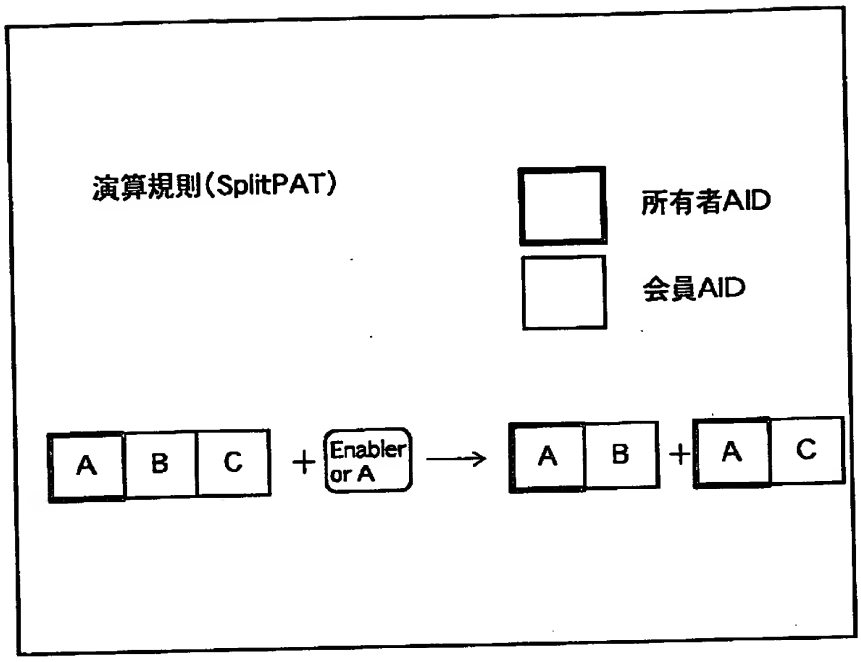
【図３３】


演算規則(MakePAT)
所有者AID
会員AID
A
B
Enabler or A
Enabler or B
A
B

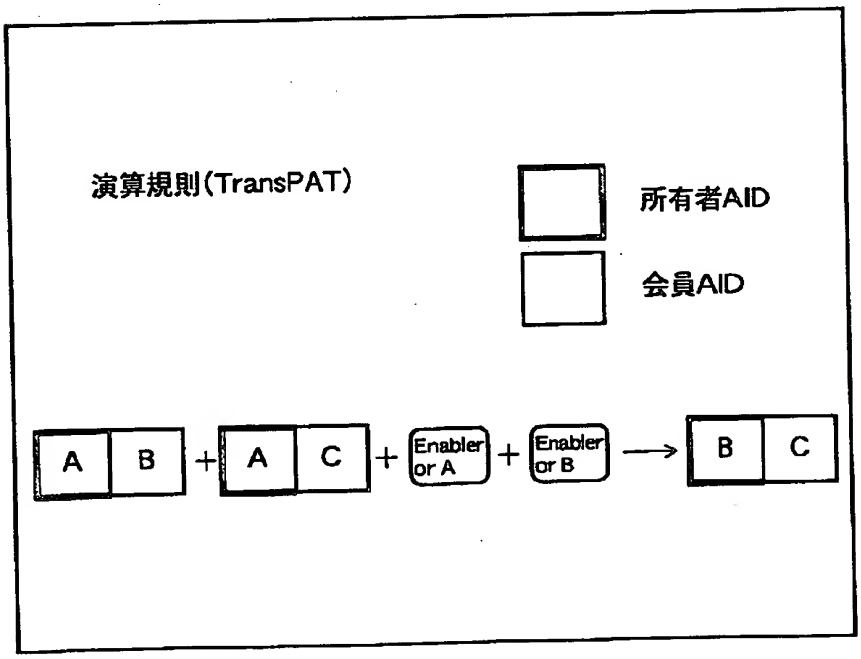
【図３４】


演算規則(MergePAT)
所有者AID
会員AID
A
B
A
C
Enabler or A
A
B
C

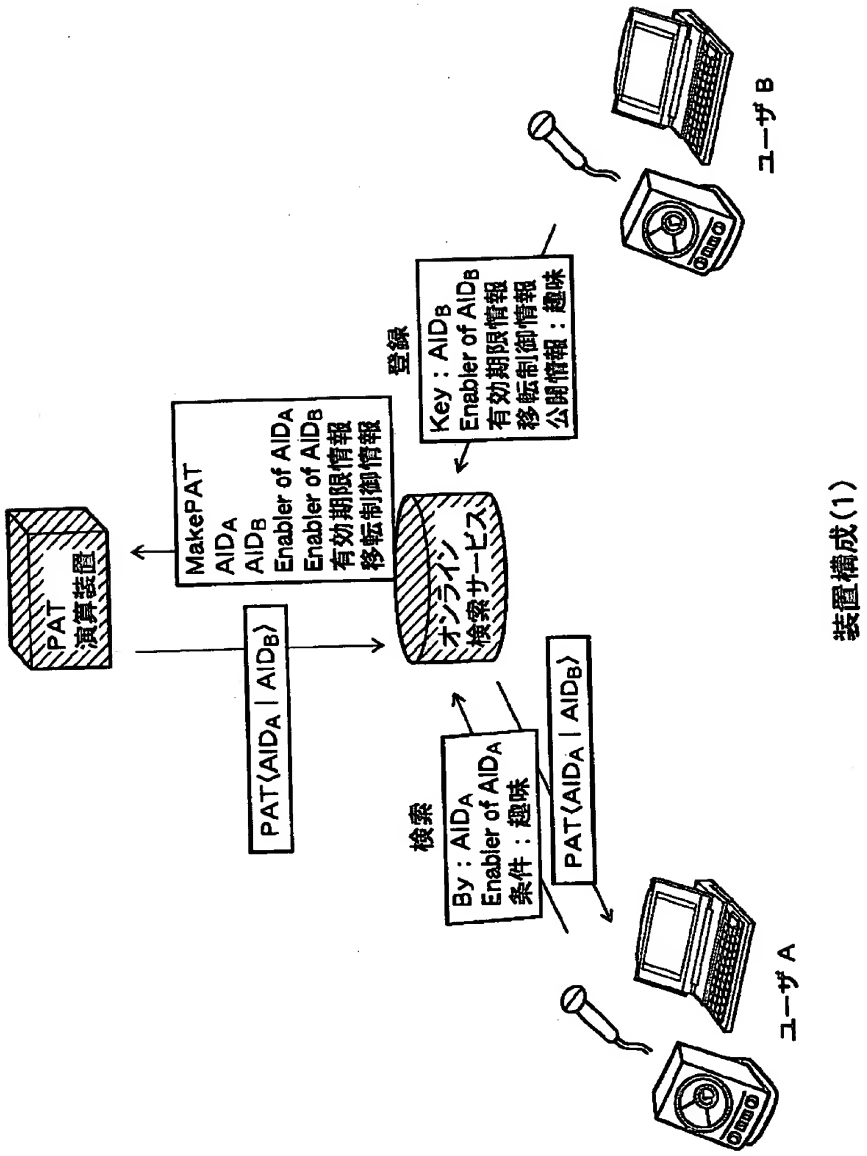
【図３５】


演算規則(SplitPAT)
所有者AID
会員AID
A
B
C
Enabler or A
A
B
A
C

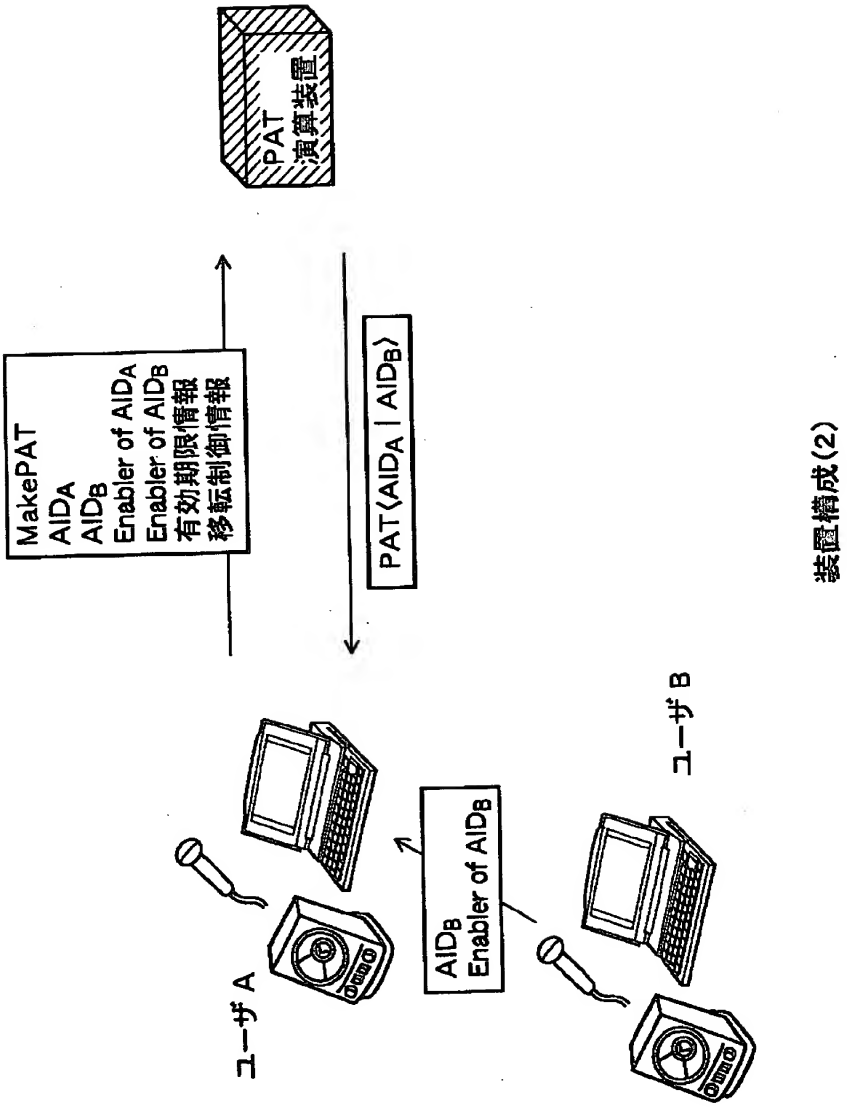
【図３６】


演算規則(TransPAT)
所有者AID
会員AID
A
B
A
C
Enabler or A
Enabler or B
B
C

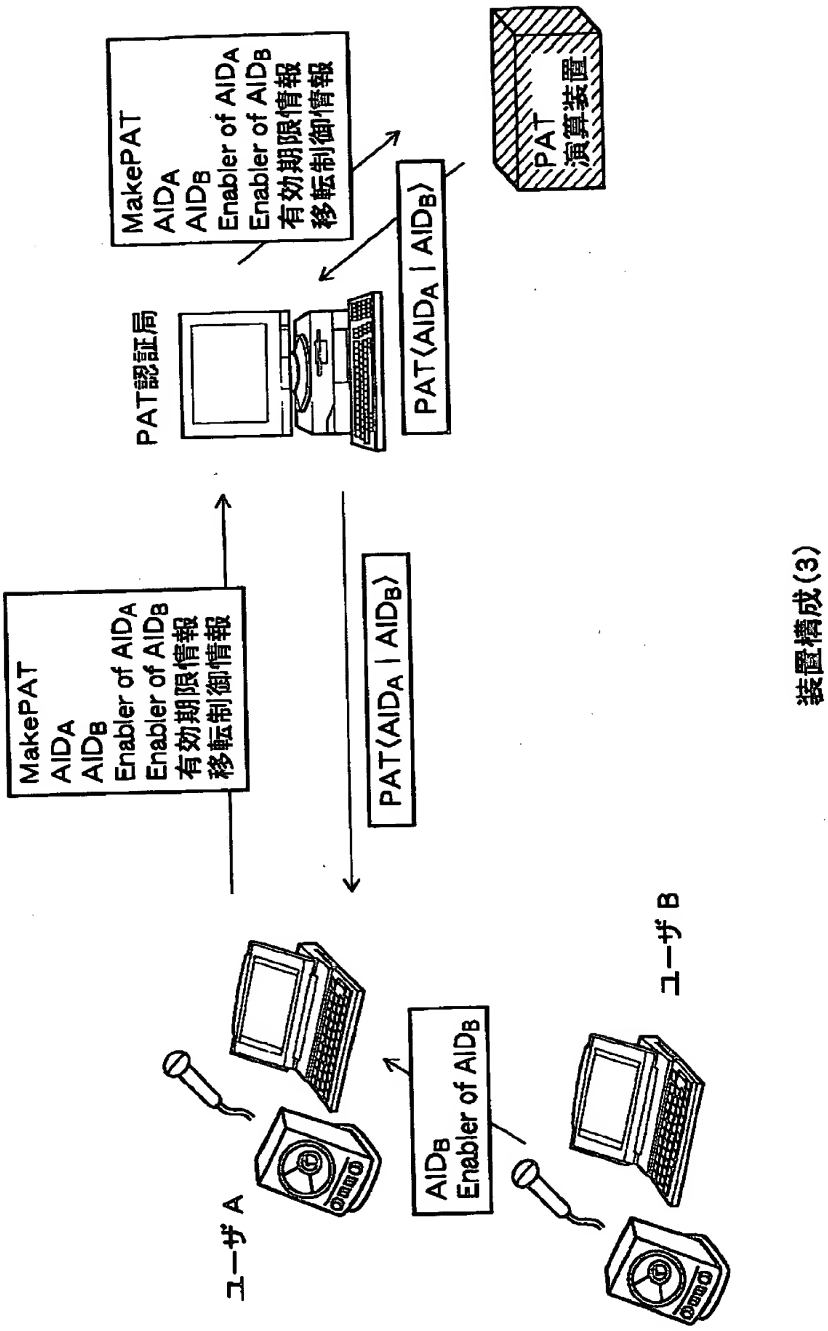
【図３７】


PAT
演算装置
MakePAT
AIDA
AIDB
EnablerofAIDA
EnablerofAIDB
有効期限情報
移転制御情報
PAT〈AIDA | AIDB〉
オンライン
検索サービス
登録
Key：AIDB
EnablerofAIDB
有効期限情報
移転制御情報
公開情報：趣味
検索
By：AIDA
EnablerofAIDA
条件：趣味
PAT〈AIDA | AIDB〉
ユーザB
ユーザA
装置構成(1)

【図３８】

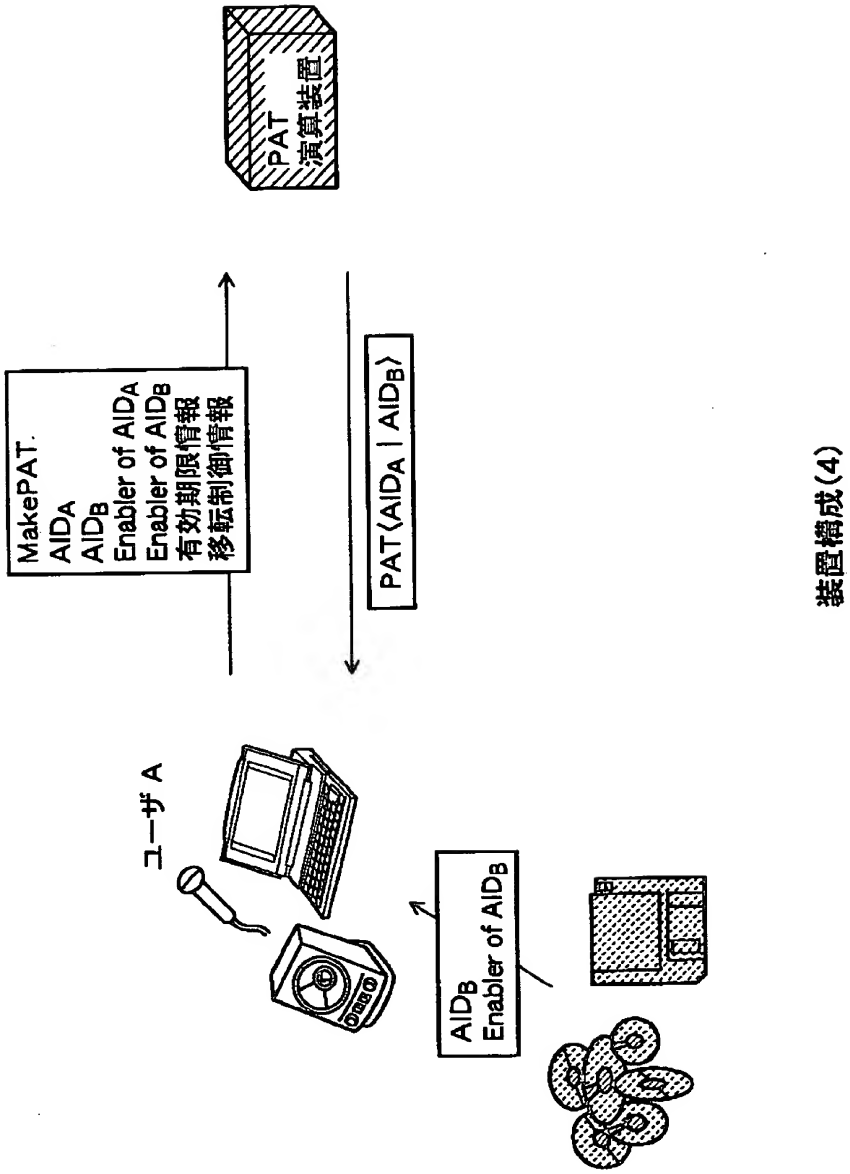

PAT
演算装置
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT〈AIDA | AIDB〉
ユーザ A
AIDB
Enabler of AIDB
ユーザ B
装置構成(2)

【図３９】

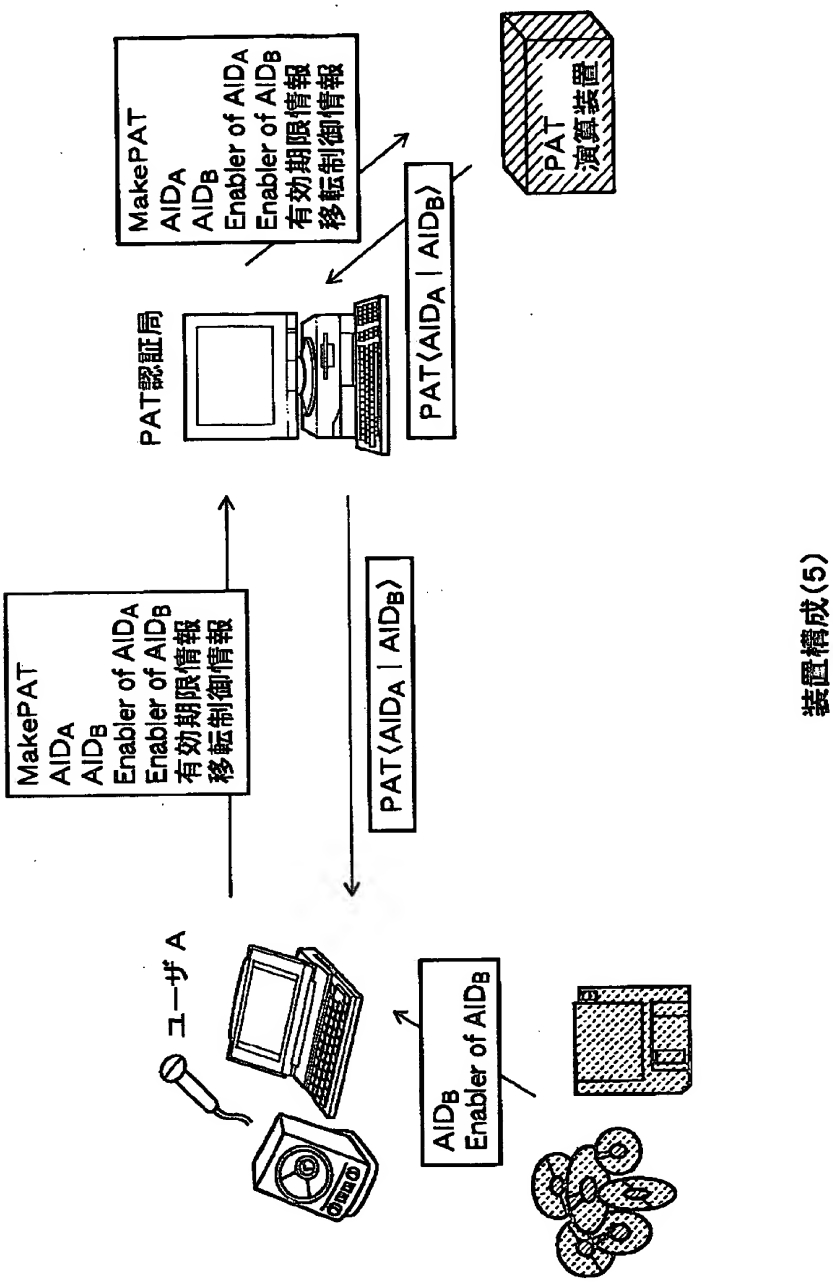

MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT
演算装置
PAT認証局
PAT(AIDA | AIDB)
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT(AIDA | AIDB)
ユーザA
AIDB
Enabler of AIDB
ユーザB

装置構成(3)

【図４０】

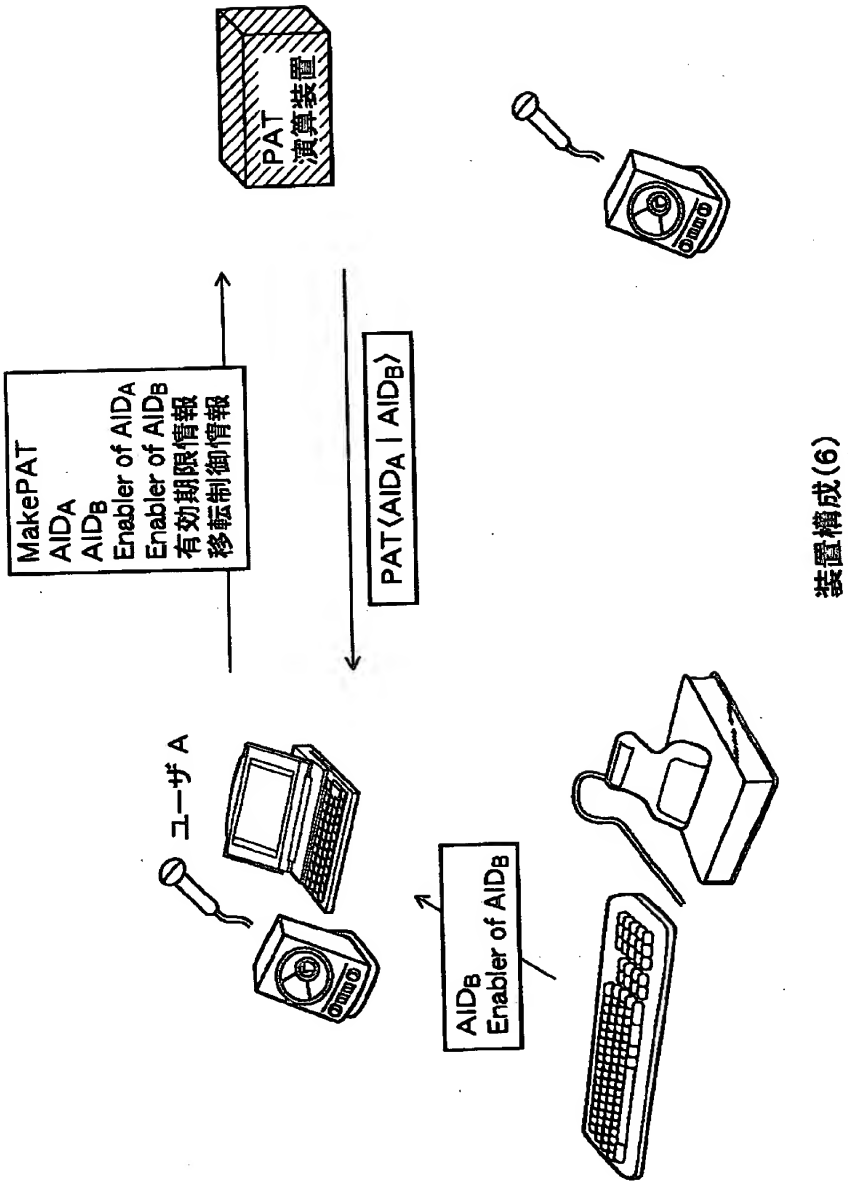

PAT
演算装置
MakePAT.
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT〈AIDA | AIDB〉
ユーザ A
AIDB
Enabler of AIDB
装置構成(4)

【図４１】

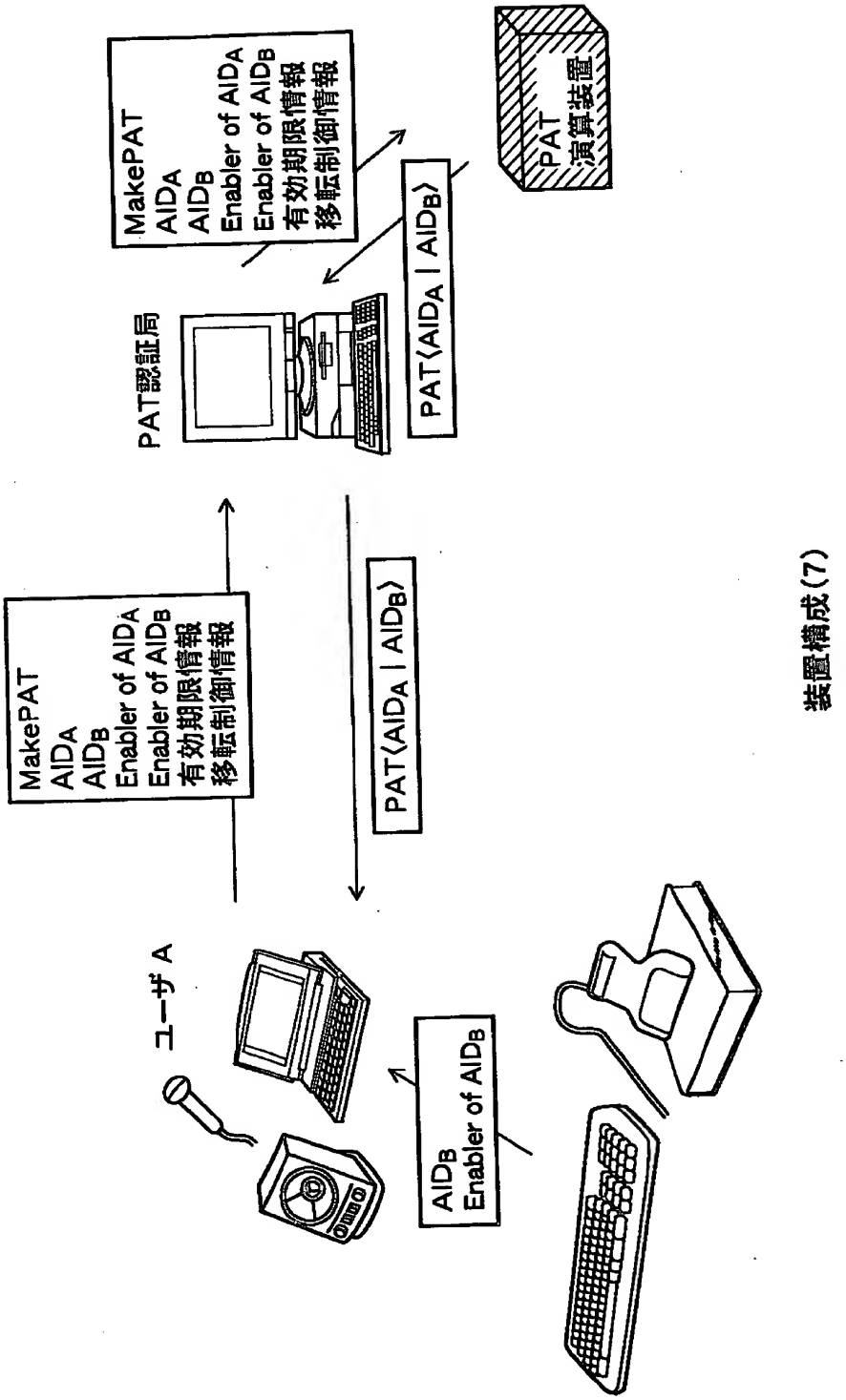

MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT
演算装置
PAT認証局
PAT〈AIDA | AIDB〉
PAT〈AIDA | AIDB〉
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
ユーザA
AIDB
Enabler of AIDB

装置構成(5)

【図４２】

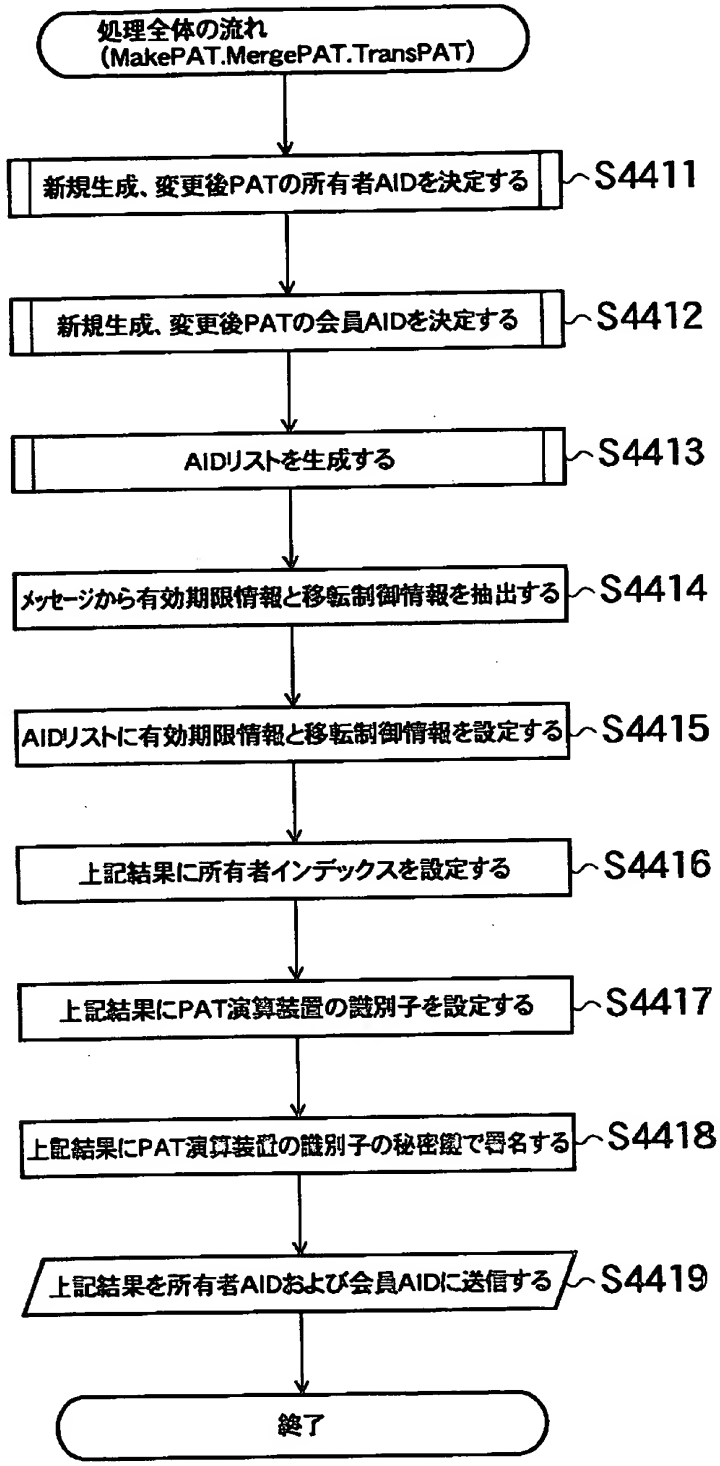

PAT
演算装置
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT〈AIDA | AIDB〉
ユーザA
AIDB
Enabler of AIDB
装置構成(6)

【図４３】

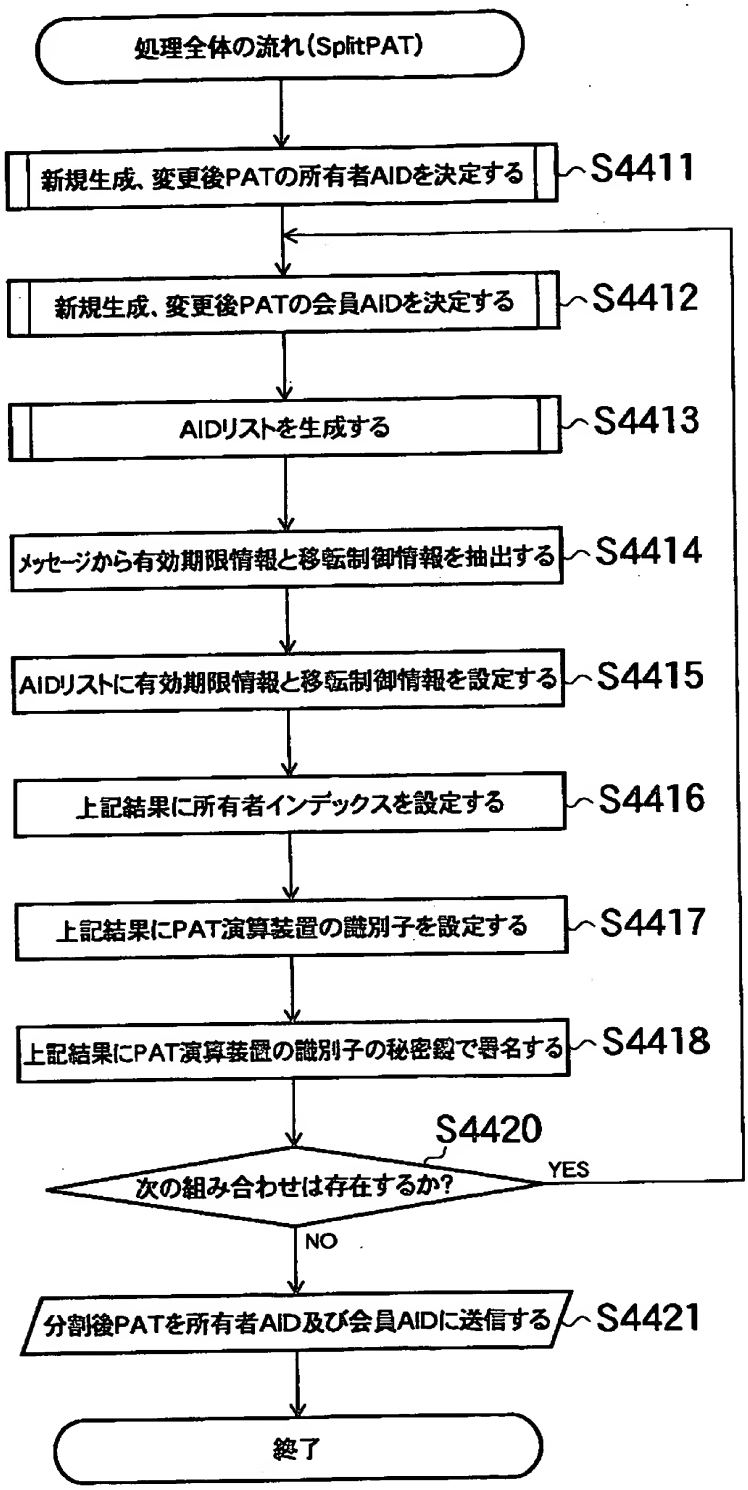

MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT
演算装置
PAT認証局
PAT〈AIDA | AIDB〉
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT〈AIDA | AIDB〉
ユーザ A
AIDB
Enabler of AIDB

装置構成(7)

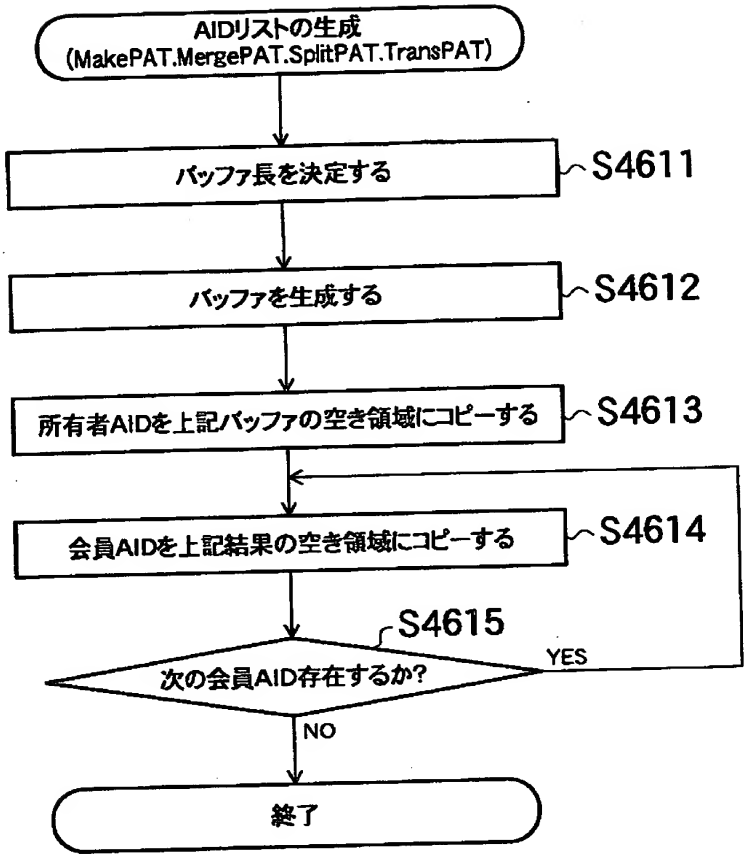
【図４４】


処理全体の流れ
(MakePAT.MergePAT.TransPAT)
新規生成、変更後PATの所有者AIDを決定する
S4411
新規生成、変更後PATの会員AIDを決定する
S4412
AIDリストを生成する
S4413
メッセージから有効期限情報と移転制御情報を抽出する
S4414
AIDリストに有効期限情報と移転制御情報を設定する
S4415
上記結果に所有者インデックスを設定する
S4416
上記結果にPAT演算装置の識別子を設定する
S4417
上記結果にPAT演算装置の識別子の秘密鍵で署名する
S4418
上記結果を所有者AIDおよび会員AIDに送信する
S4419
終了

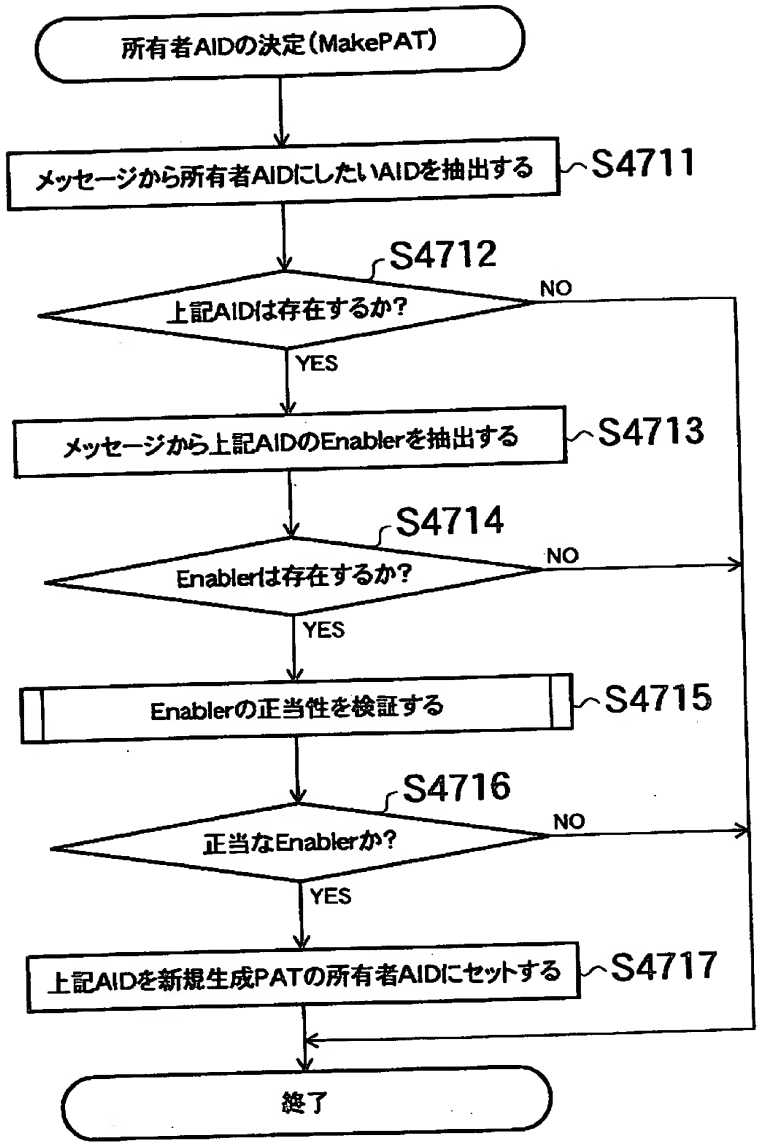
【図４５】


処理全体の流れ(SplitPAT)
新規生成、変更後PATの所有者AIDを決定する
S4411
新規生成、変更後PATの会員AIDを決定する
S4412
AIDリストを生成する
S4413
メッセージから有効期限情報と移転制御情報を抽出する
S4414
AIDリストに有効期限情報と移転制御情報を設定する
S4415
上記結果に所有者インデックスを設定する
S4416
上記結果にPAT演算装置の識別子を設定する
S4417
上記結果にPAT演算装置の識別子の秘密鍵で署名する
S4418
S4420
次の組み合わせは存在するか?
YES
NO
分割後PATを所有者AID及び会員AIDに送信する
S4421
終了

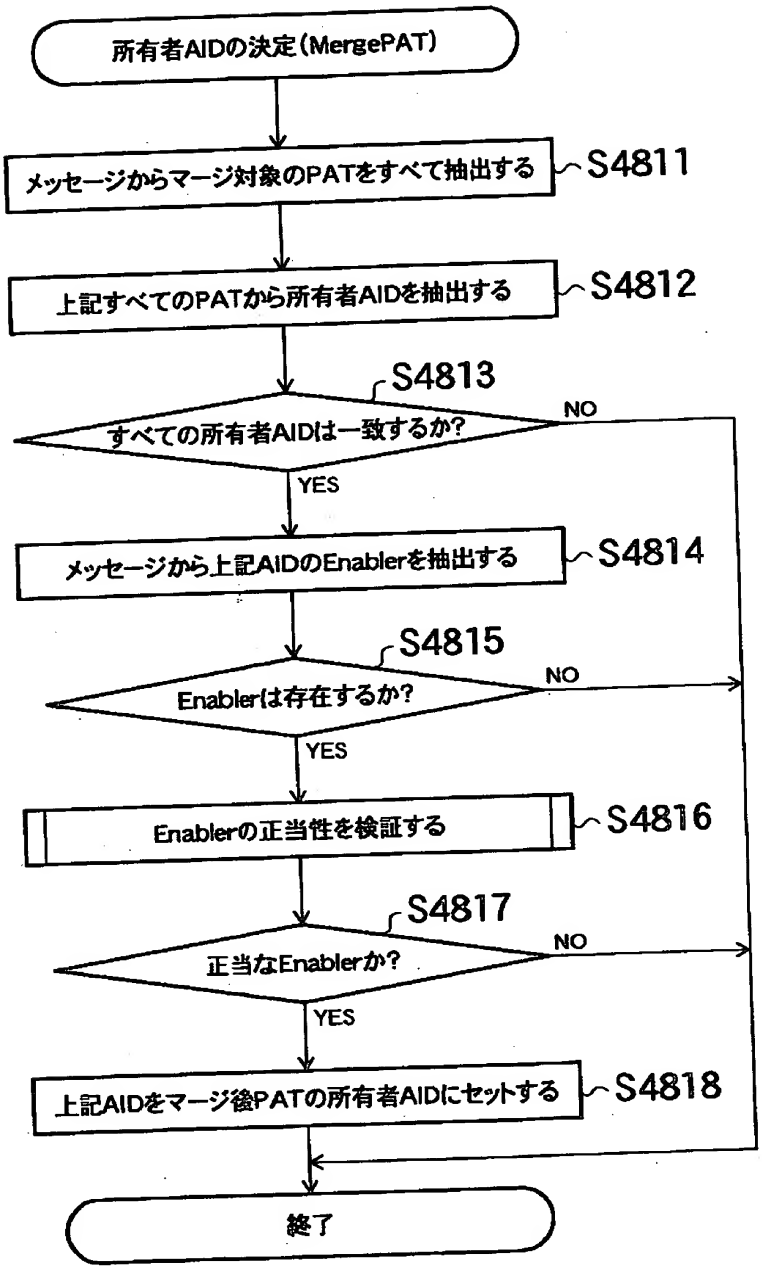
【図４６】


AIDリストの生成
(MakePAT.MergePAT.SplitPAT.TransPAT)
バッファ長を決定する
S4611
バッファを生成する
S4612
所有者AIDを上記バッファの空き領域にコピーする
S4613
会員AIDを上記結果の空き領域にコピーする
S4614
S4615
次の会員AID存在するか?
YES
NO
終了

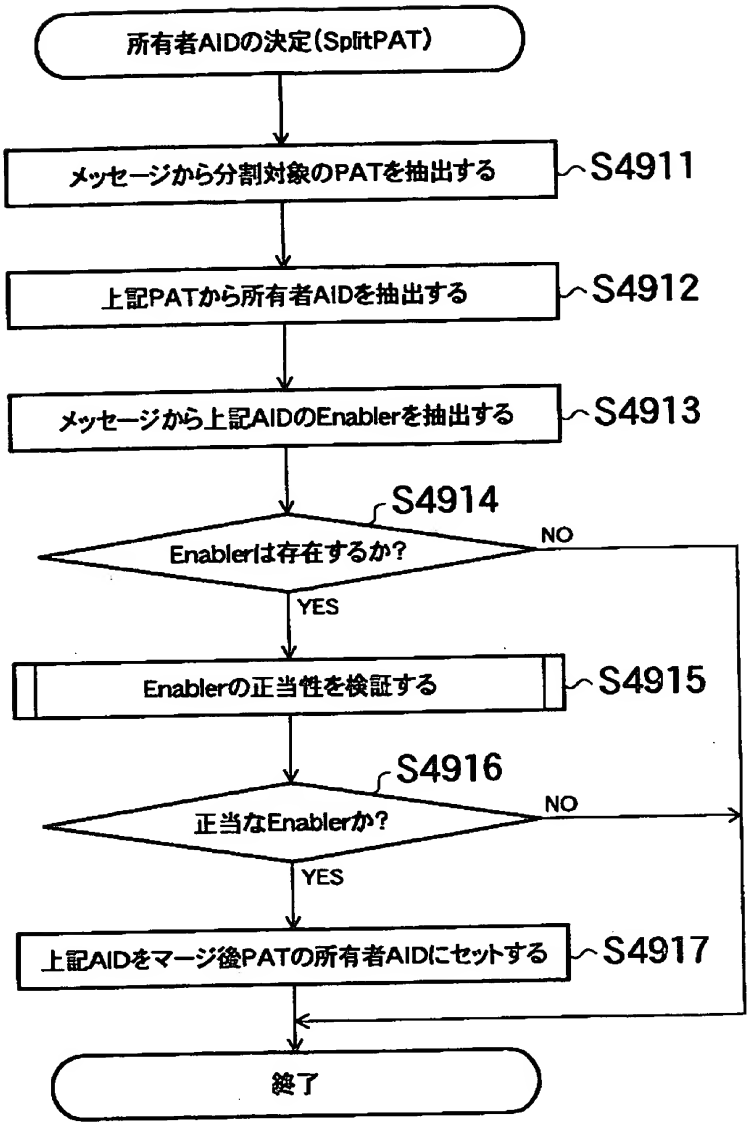
【図４７】


所有者AIDの決定(MakePAT)
メッセージから所有者AIDにしたいAIDを抽出する
S4711
S4712
上記AIDは存在するか?
NO
YES
メッセージから上記AIDのEnablerを抽出する
S4713
S4714
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S4715
S4716
正当なEnablerか?
NO
YES
上記AIDを新規生成PATの所有者AIDにセットする
S4717
終了

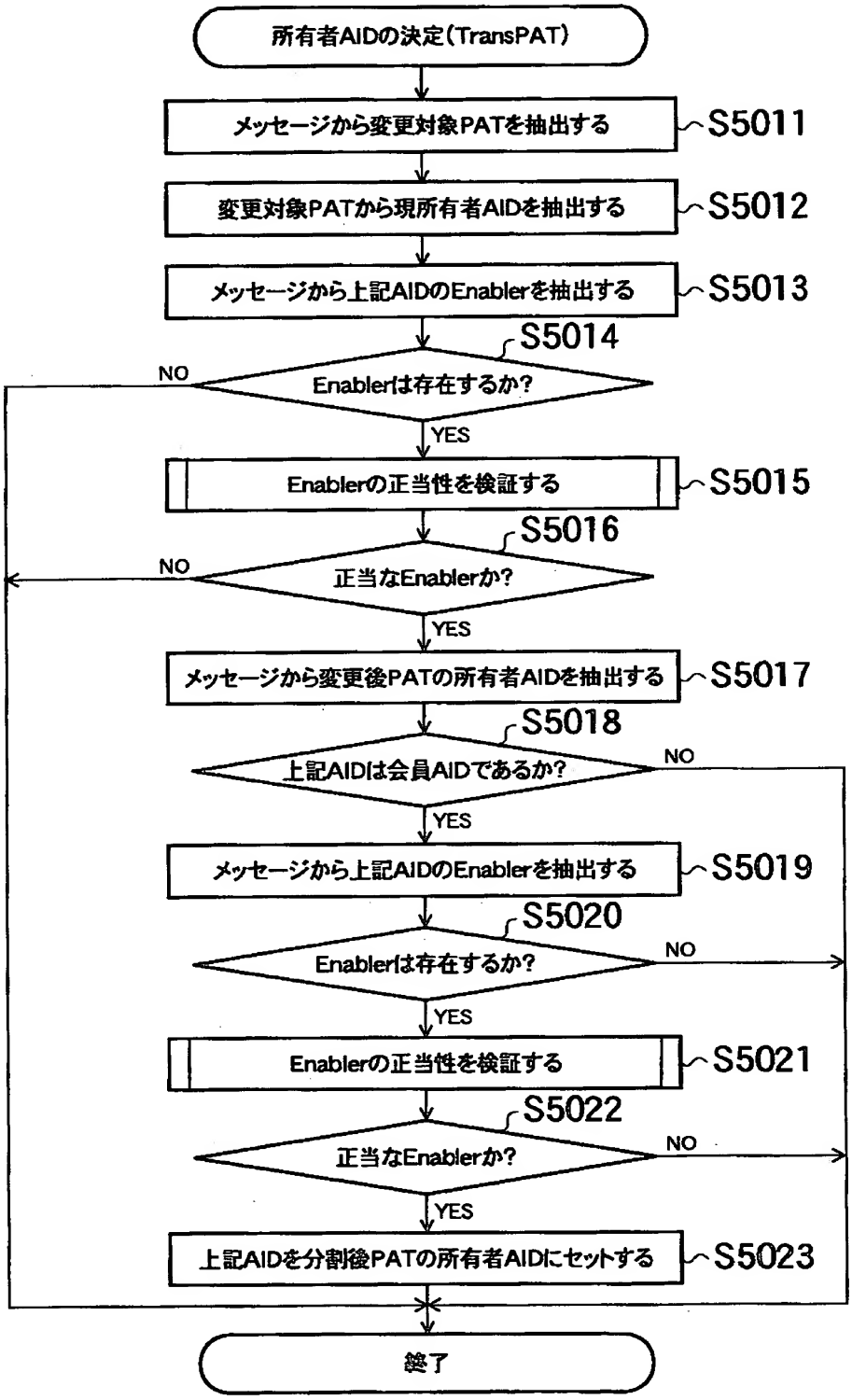
【図４８】


所有者AIDの決定(MergePAT)
メッセージからマージ対象のPATをすべて抽出する
S4811
上記すべてのPATから所有者AIDを抽出する
S4812
S4813
すべての所有者AIDは一致するか?
NO
YES
メッセージから上記AIDのEnablerを抽出する
S4814
S4815
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S4816
S4817
正当なEnablerか?
NO
YES
上記AIDをマージ後PATの所有者AIDにセットする
S4818
終了

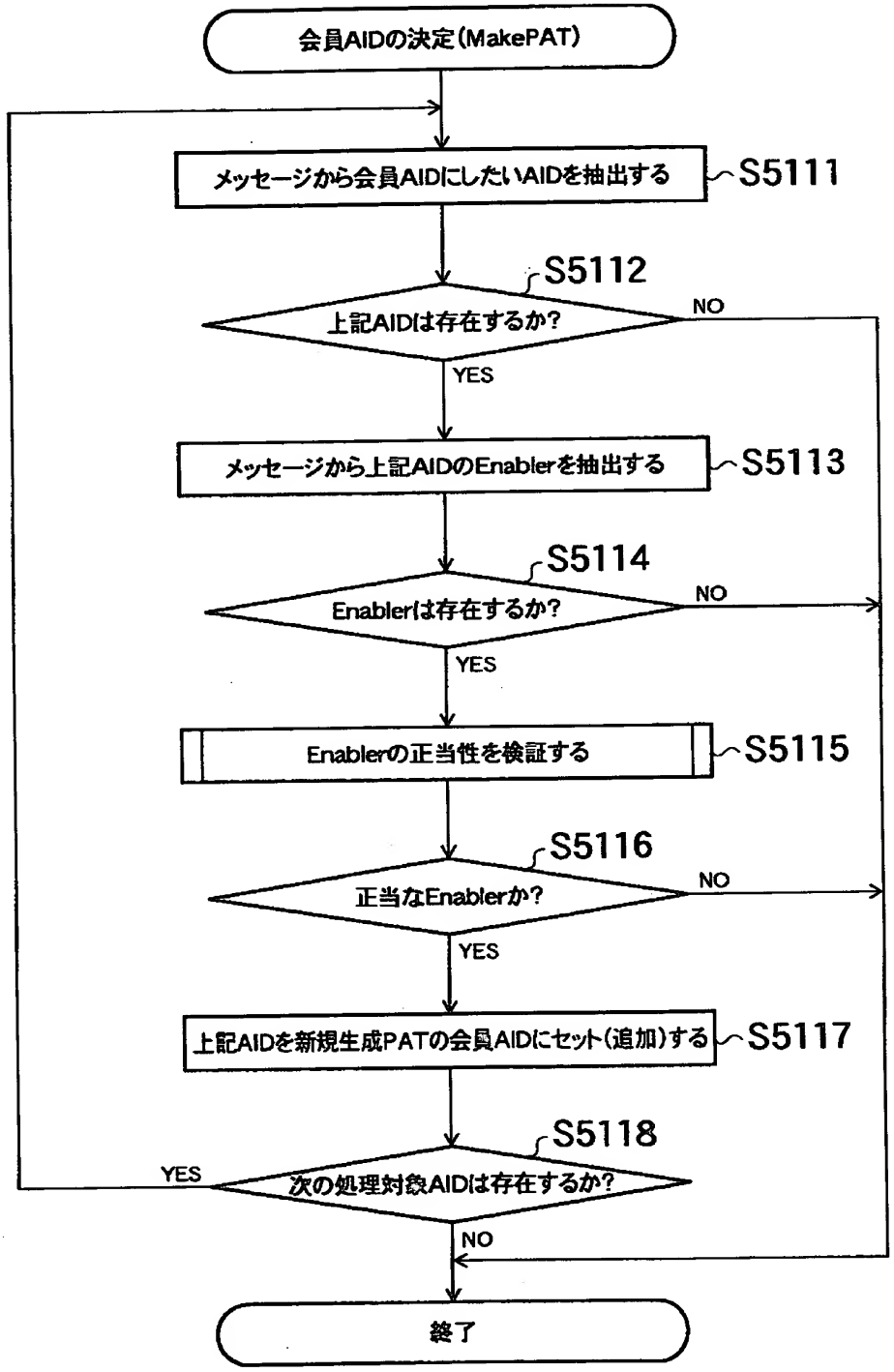
【図４９】


所有者AIDの決定(SplitPAT)
メッセージから分割対象のPATを抽出する
S4911
上記PATから所有者AIDを抽出する
S4912
メッセージから上記AIDのEnablerを抽出する
S4913
S4914
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S4915
S4916
正当なEnablerか?
NO
YES
上記AIDをマージ後PATの所有者AIDにセットする
S4917
終了

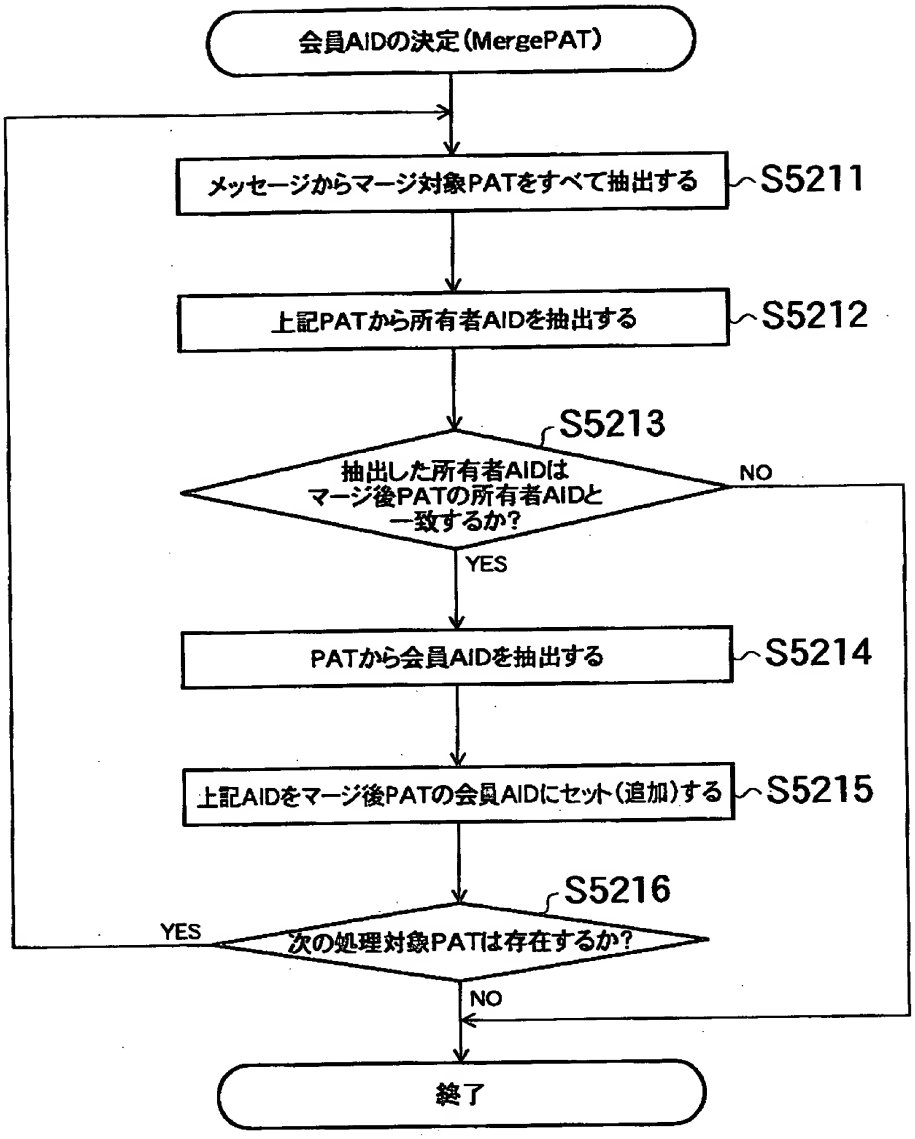
【図５０】


所有者AIDの決定(TransPAT)
メッセージから変更対象PATを抽出する
S5011
変更対象PATから現所有者AIDを抽出する
S5012
メッセージから上記AIDのEnablerを抽出する
S5013
S5014
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S5015
S5016
正当なEnablerか?
NO
YES
メッセージから変更後PATの所有者AIDを抽出する
S5017
S5018
上記AIDは会員AIDであるか?
NO
YES
メッセージから上記AIDのEnablerを抽出する
S5019
S5020
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S5021
S5022
正当なEnablerか?
NO
YES
上記AIDを分割後PATの所有者AIDにセットする
S5023
終了

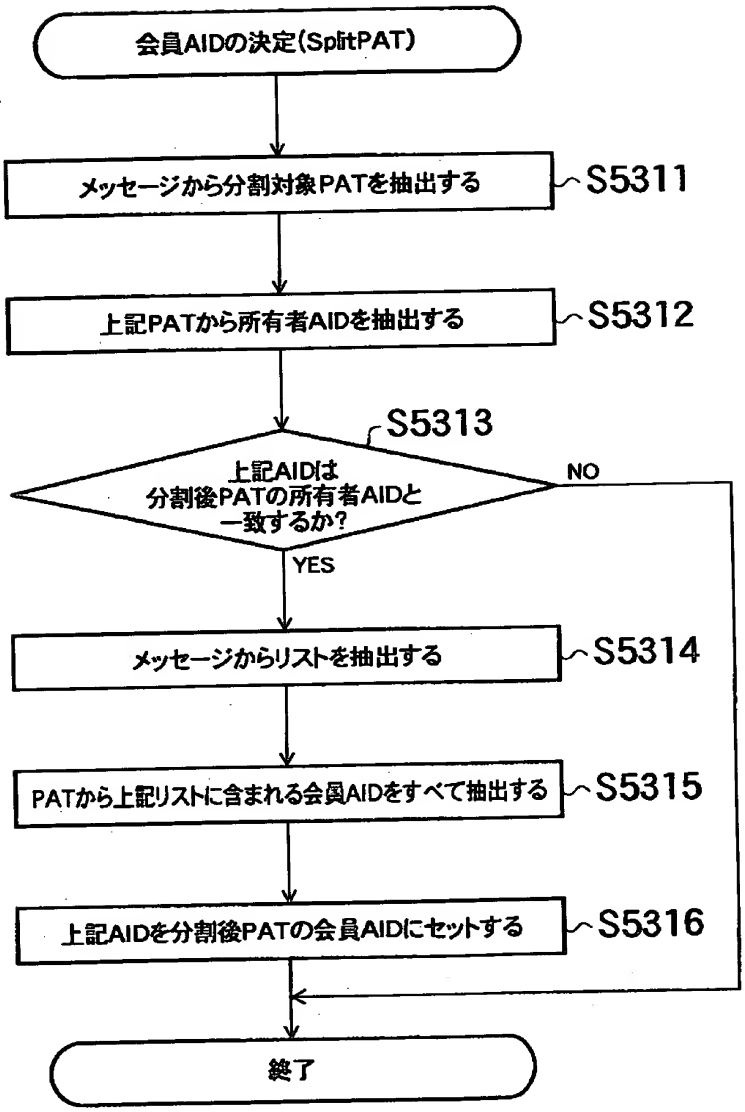
【図５１】


会員AIDの決定(MakePAT)
メッセージから会員AIDにしたいAIDを抽出する
S5111
S5112
上記AIDは存在するか?
NO
YES
メッセージから上記AIDのEnablerを抽出する
S5113
S5114
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S5115
S5116
正当なEnablerか?
NO
YES
上記AIDを新規生成PATの会員AIDにセット(追加)する
S5117
S5118
YES
次の処理対象AIDは存在するか?
NO
終了

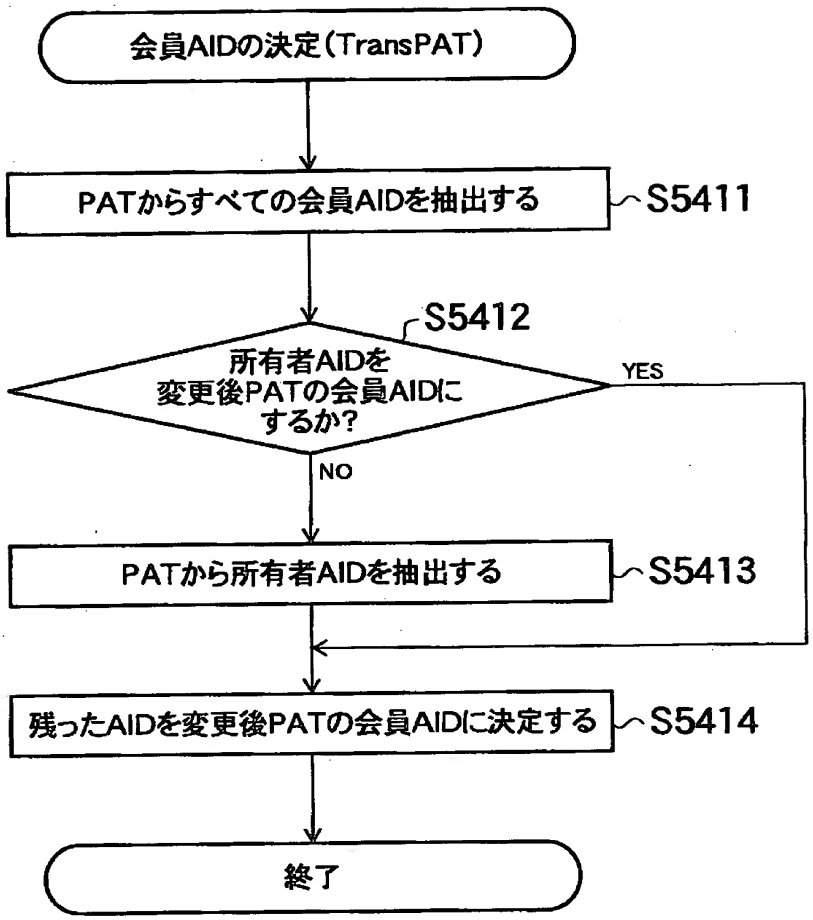
【図５２】


会員AIDの決定(MergePAT)
メッセージからマージ対象PATをすべて抽出する
S5211
上記PATから所有者AIDを抽出する
S5212
S5213
抽出した所有者AIDは
マージ後PATの所有者AIDと
一致するか?
NO
YES
PATから会員AIDを抽出する
S5214
上記AIDをマージ後PATの会員AIDにセット(追加)する
S5215
S5216
YES
次の処理対象PATは存在するか?
NO
終了

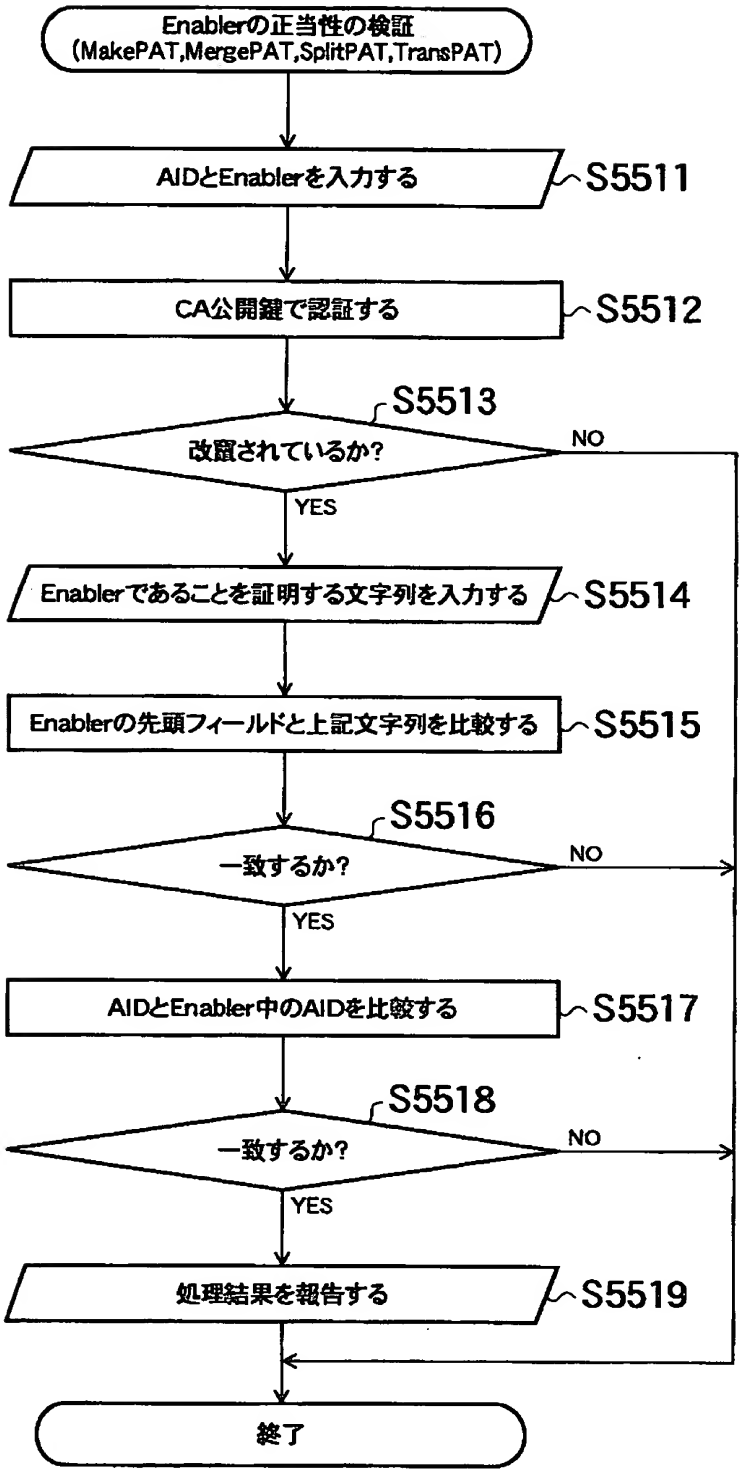
【図５３】


会員AIDの決定(SplitPAT)
メッセージから分割対象PATを抽出する
S5311
上記PATから所有者AIDを抽出する
S5312
S5313
上記AIDは
分割後PATの所有者AIDと
一致するか?
NO
YES
メッセージからリストを抽出する
S5314
PATから上記リストに含まれる会員AIDをすべて抽出する
S5315
上記AIDを分割後PATの会員AIDにセットする
S5316
終了

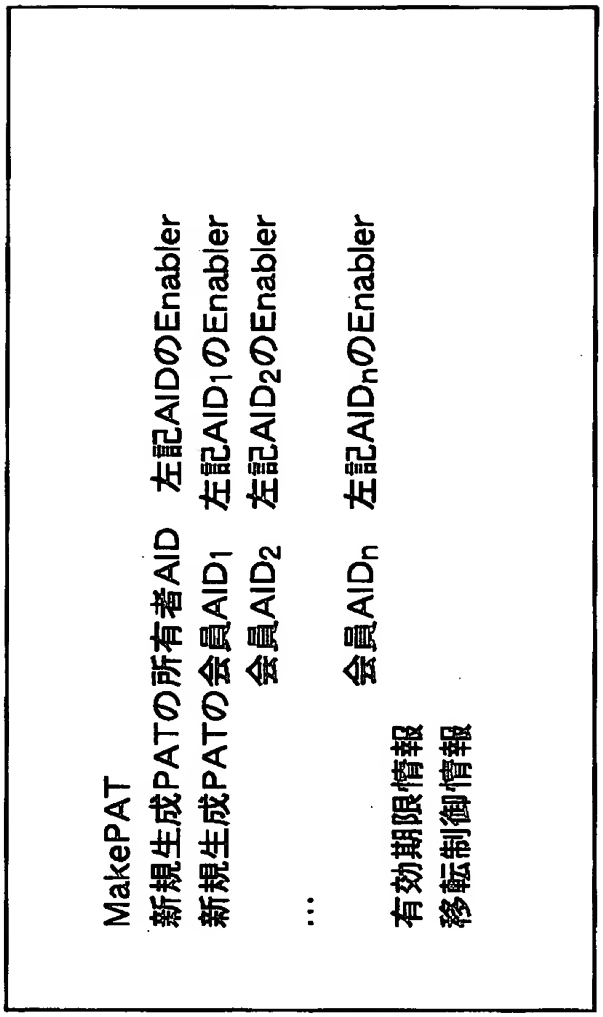
【図５４】


会員AIDの決定(TransPAT)
PATからすべての会員AIDを抽出する
S5411
S5412
所有者AIDを
変更後PATの会員AIDに
するか?
YES
NO
PATから所有者AIDを抽出する
S5413
残ったAIDを変更後PATの会員AIDに決定する
S5414
終了

【図５５】


Enablerの正当性の検証
(MakePAT,MergePAT,SplitPAT,TransPAT)
AIDとEnablerを入力する
S5511
CA公開鍵で認証する
S5512
S5513
改竄されているか?
NO
YES
Enablerであることを証明する文字列を入力する
S5514
Enablerの先頭フィールドと上記文字列を比較する
S5515
S5516
一致するか?
NO
YES
AIDとEnabler中のAIDを比較する
S5517
S5518
一致するか?
NO
YES
処理結果を報告する
S5519
終了

【図５６】


MakePAT命令を含むメッセージ
MakePAT
新規生成PATの所有者AID　左記AIDのEnabler
新規生成PATの会員AID1　左記AID1のEnabler
会員AID2　左記AID2のEnabler
…
会員AIDn　左記AIDnのEnabler
有効期限情報
移転制御情報

【図５７】

MergePAT命令を含むメッセージ

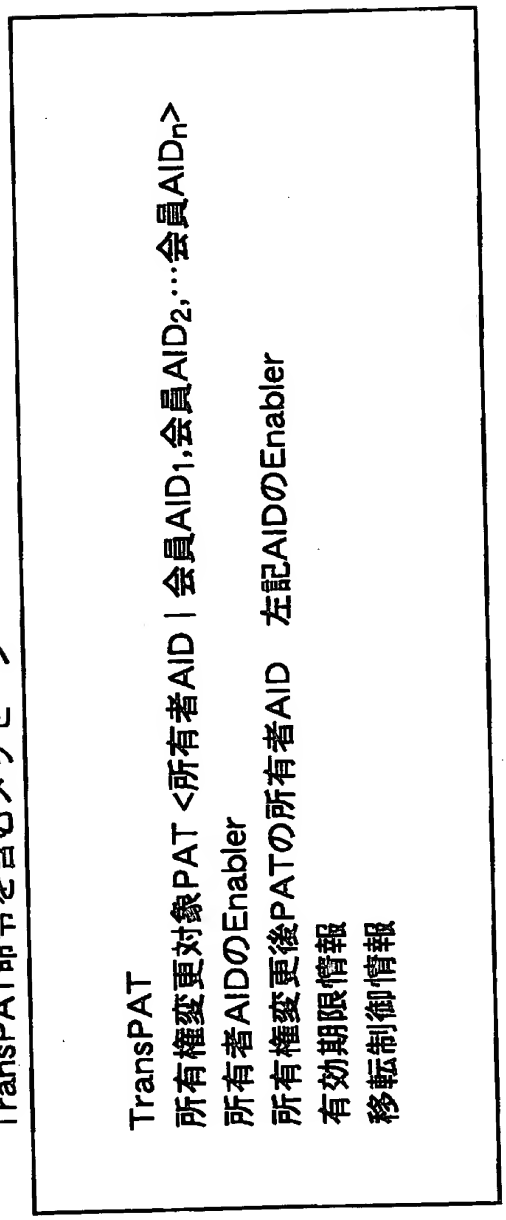
MergePAT
マージ対象PAT <所有者AID | 会員AID_{11},会員AID_{12}…会員AID_{1n}>
マージ対象PAT <所有者AID | 会員AID_{21},会員AID_{22}…会員AID_{2n}>
…
マージ対象PAT <所有者AID | 会員AID_{m1},会員AID_{m2}…会員AID_{mn}>
マージ後PATの所有者AIDのEnabler
有効期限情報
移転制御情報

【図５８】

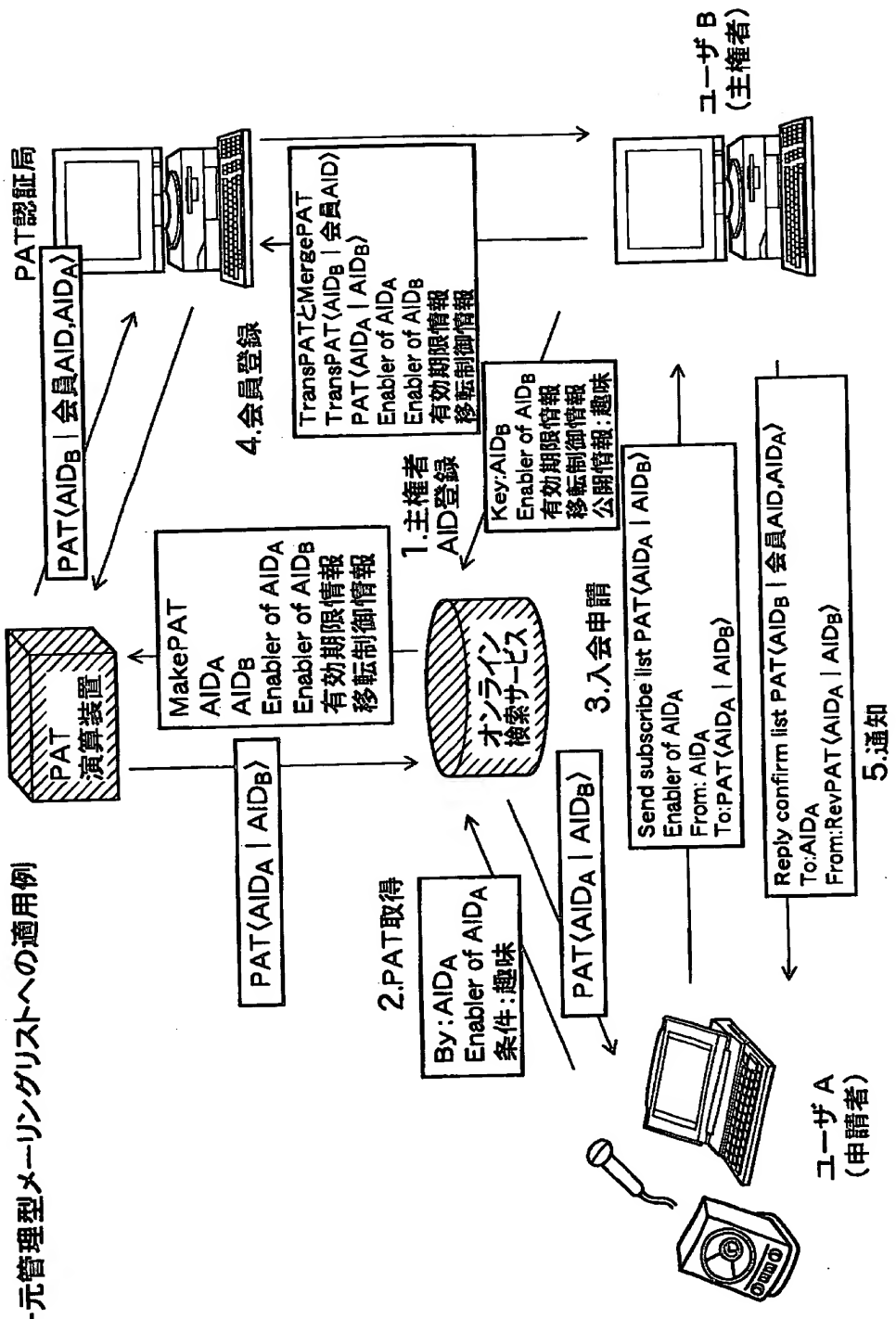
SplitPAT命令を含むメッセージ

SplitPAT
分割対象PAT <所有者AID | 会員AID_1,会員AID_2…会員AID_n>
組み合わせ$_1$（会員AID_1,会員AID_3,有効期限情報$_1$,移転制御情報$_1$）
組み合わせ$_2$（会員AID_2,会員AID_5,有効期限情報$_2$,移転制御情報$_2$）
…
組み合わせ$_n$（会員AID_k,会員AID_l,有効期限情報$_n$,移転制御情報$_n$）
分割後PATの所有者AIDのEnabler

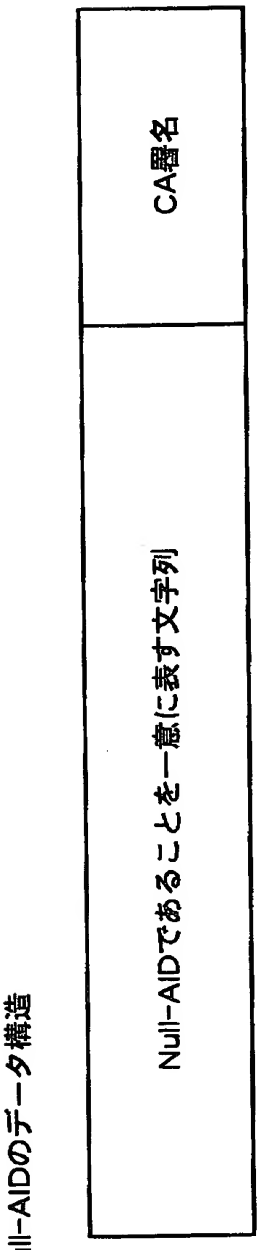
【図５９】


TransPAT命令を含むメッセージ
TransPAT
所有権変更対象PAT <所有者AID | 会員AID1,会員AID2,…会員AIDn>
所有者AIDのEnabler
所有権変更後PATの所有者AID　左記AIDのEnabler
有効期限情報
移転制御情報

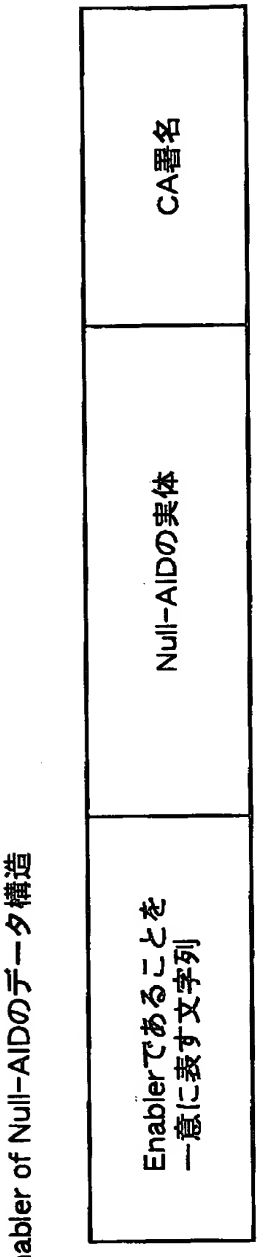
【図６０】


一元管理型メーリングリストへの適用例
PAT
演算装置
PAT認証局
ユーザ B
(主権者)
ユーザ A
(申請者)
オンライン
検索サービス
PAT〈AIDB | 会員AID,AIDA〉
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
1.主権者
AID登録
Key:AIDB
Enabler of AIDB
有効期限情報
移転制御情報
公開情報:趣味
4.会員登録
TransPATとMergePAT
TransPAT〈AIDB | 会員AID〉
PAT〈AIDA | AIDB〉
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT〈AIDA | AIDB〉
2.PAT取得
By:AIDA
Enabler of AIDA
条件:趣味
PAT〈AIDA | AIDB〉
3.入会申請
Send subscribe list PAT〈AIDA | AIDB〉
Enabler of AIDA
From: AIDA
To:PAT〈AIDA | AIDB〉
Reply confirm list PAT〈AIDB | 会員AID,AIDA〉
To:AIDA
From:RevPAT〈AIDA | AIDB〉
5.通知

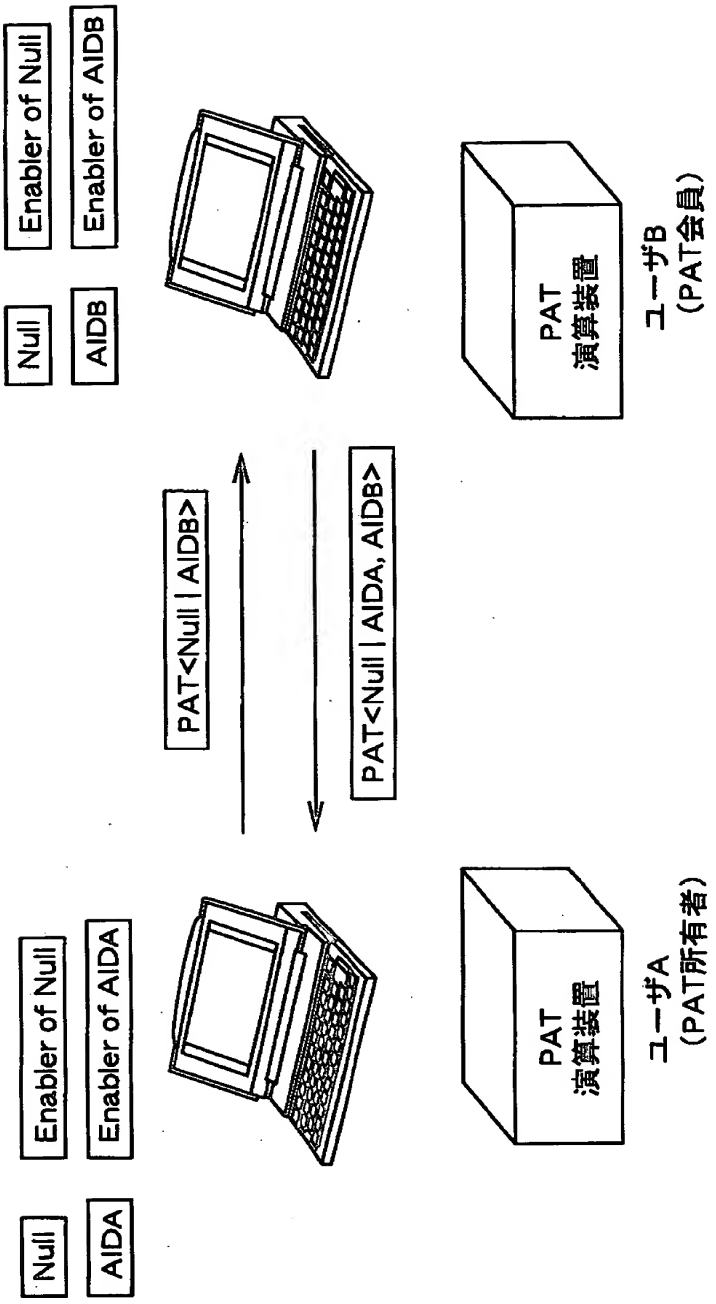
【図６１】



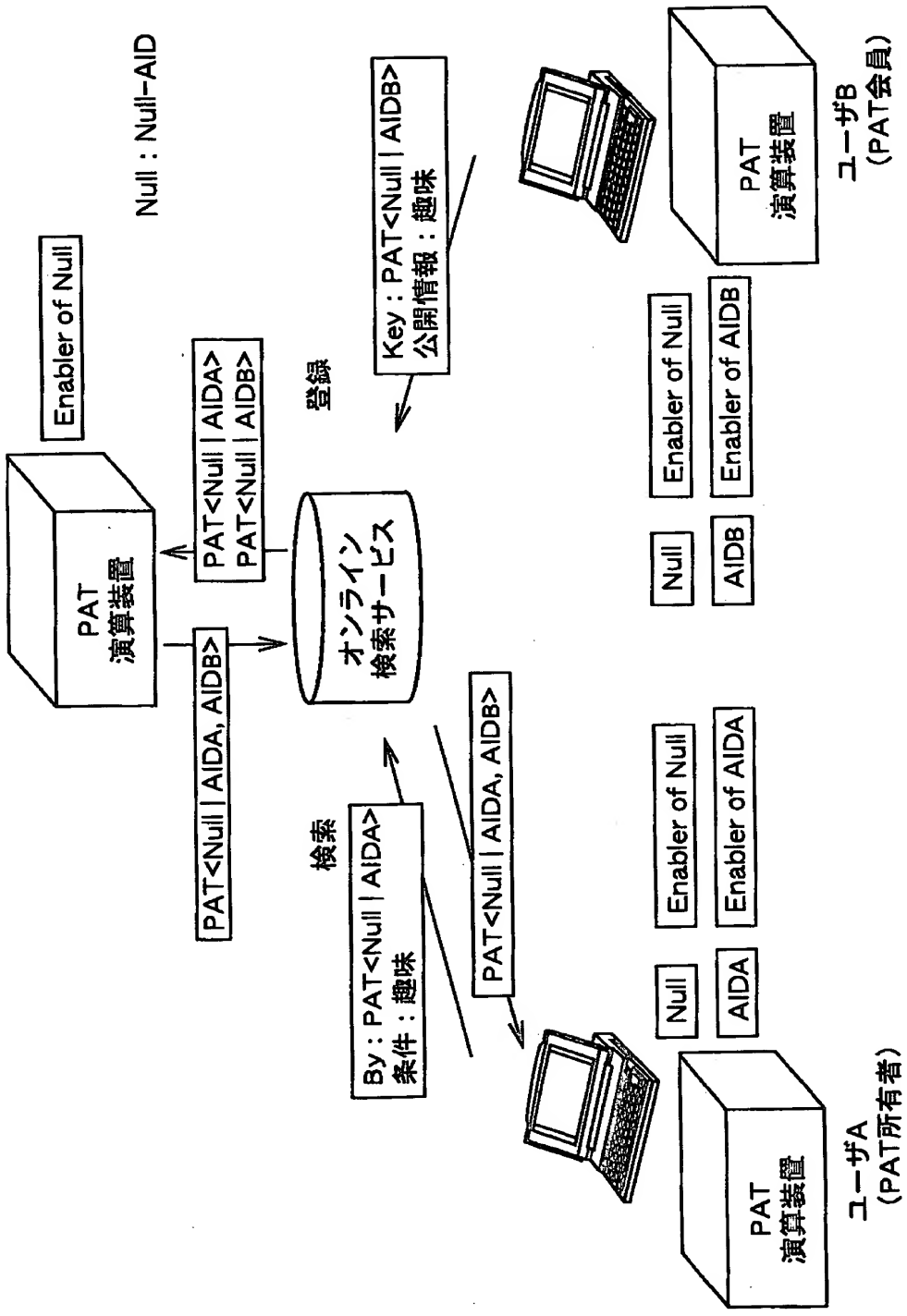
【図６２】


Enabler of Null-AIDのデータ構造
Enablerであることを
一意に表す文字列
Null-AIDの実体
CA署名

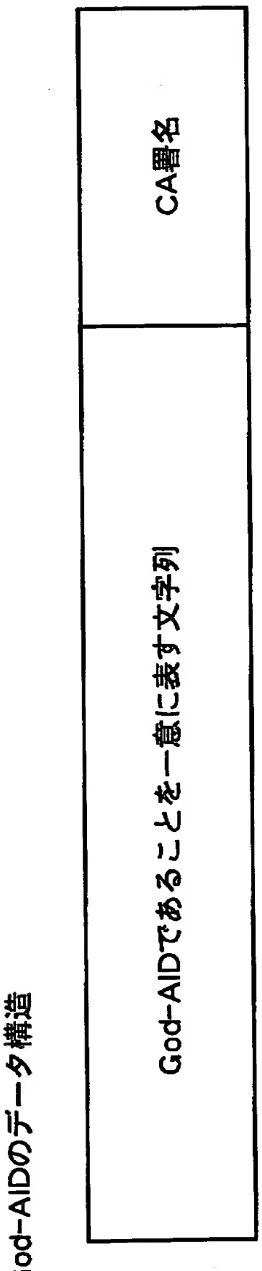
【図６３】


Enabler of Null
Enabler of AIDB
Null
AIDB
PAT
演算装置
ユーザB
(PAT会員)
PAT<Null | AIDB>
PAT<Null | AIDA, AIDB>
Enabler of Null
Enabler of AIDA
Null
AIDA
PAT
演算装置
ユーザA
(PAT所有者)

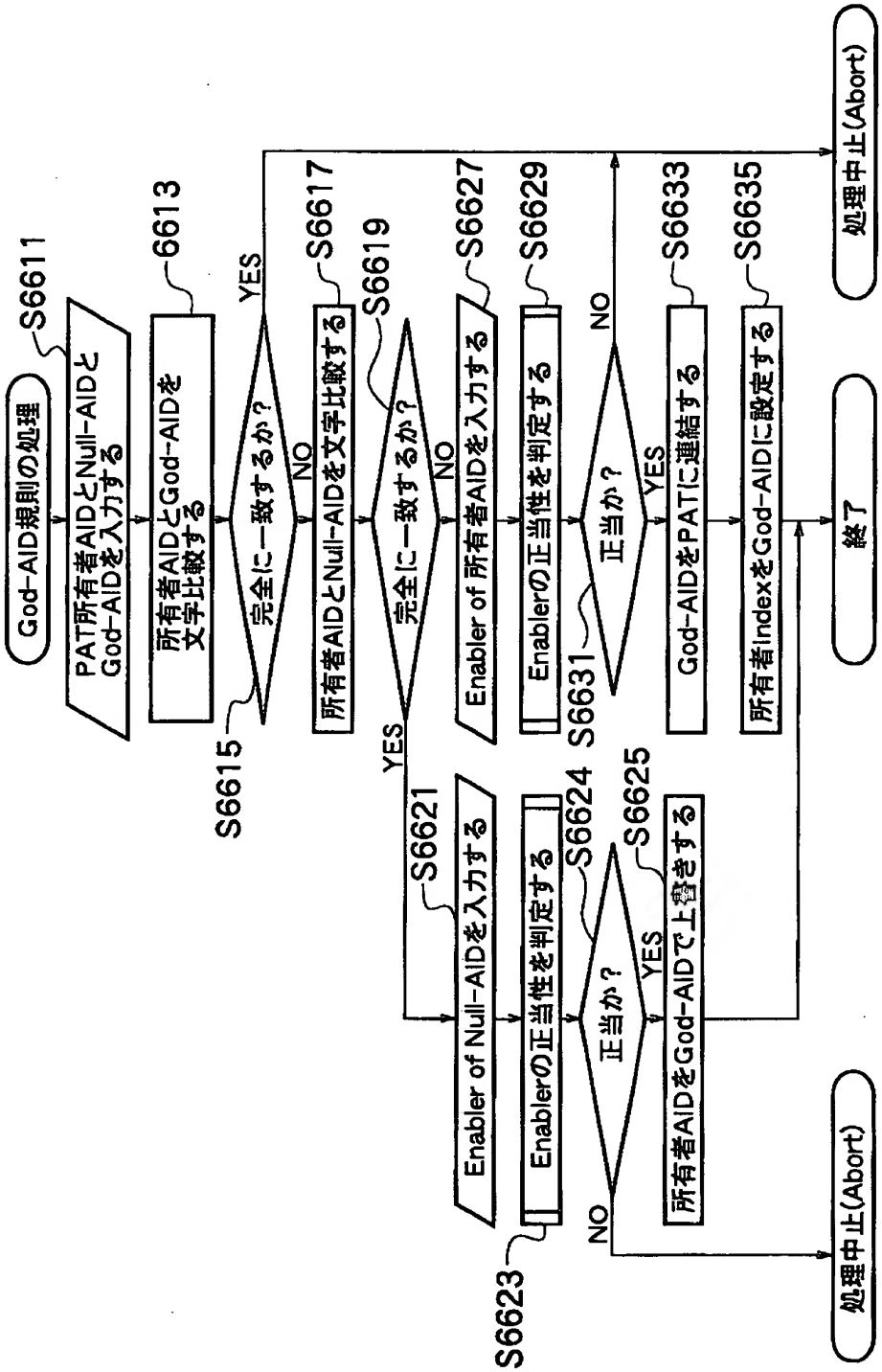
【図６４】


Null : Null=AID
Enabler of Null
PAT
演算装置
PAT<Null | AIDA>
PAT<Null | AIDB>
登録
PAT<Null | AIDA, AIDB>
オンライン
検索サービス
Key : PAT<Null | AIDB>
公開情報 : 趣味
検索
By : PAT<Null | AIDA>
条件 : 趣味
PAT<Null | AIDA, AIDB>
Null
AIDB
Enabler of Null
Enabler of AIDB
PAT
演算装置
ユーザB
(PAT会員)
Null
AIDA
Enabler of Null
Enabler of AIDA
PAT
演算装置
ユーザA
(PAT所有者)

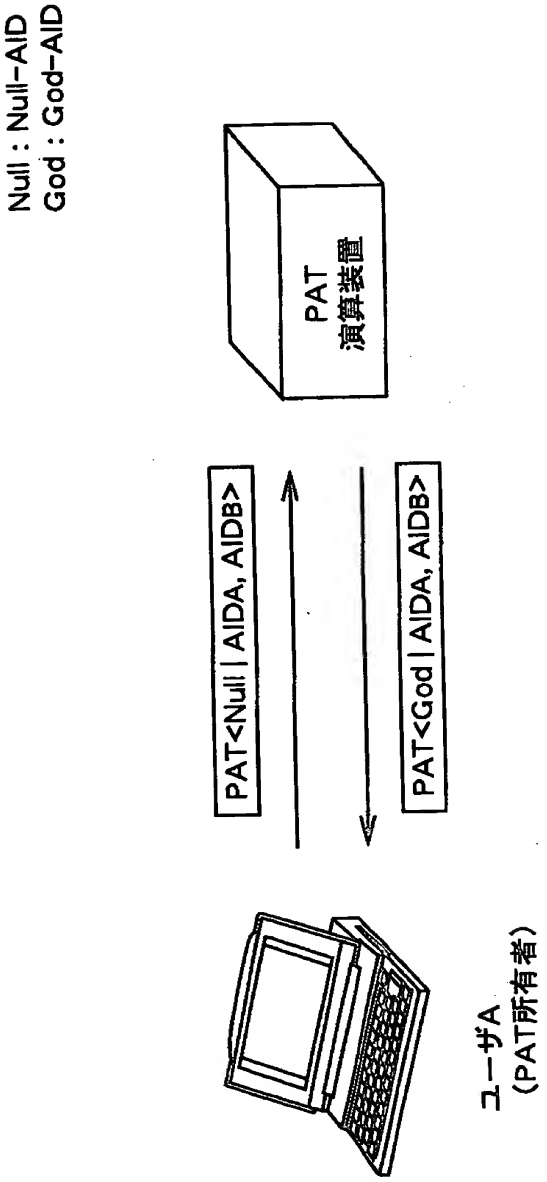
【図６５】



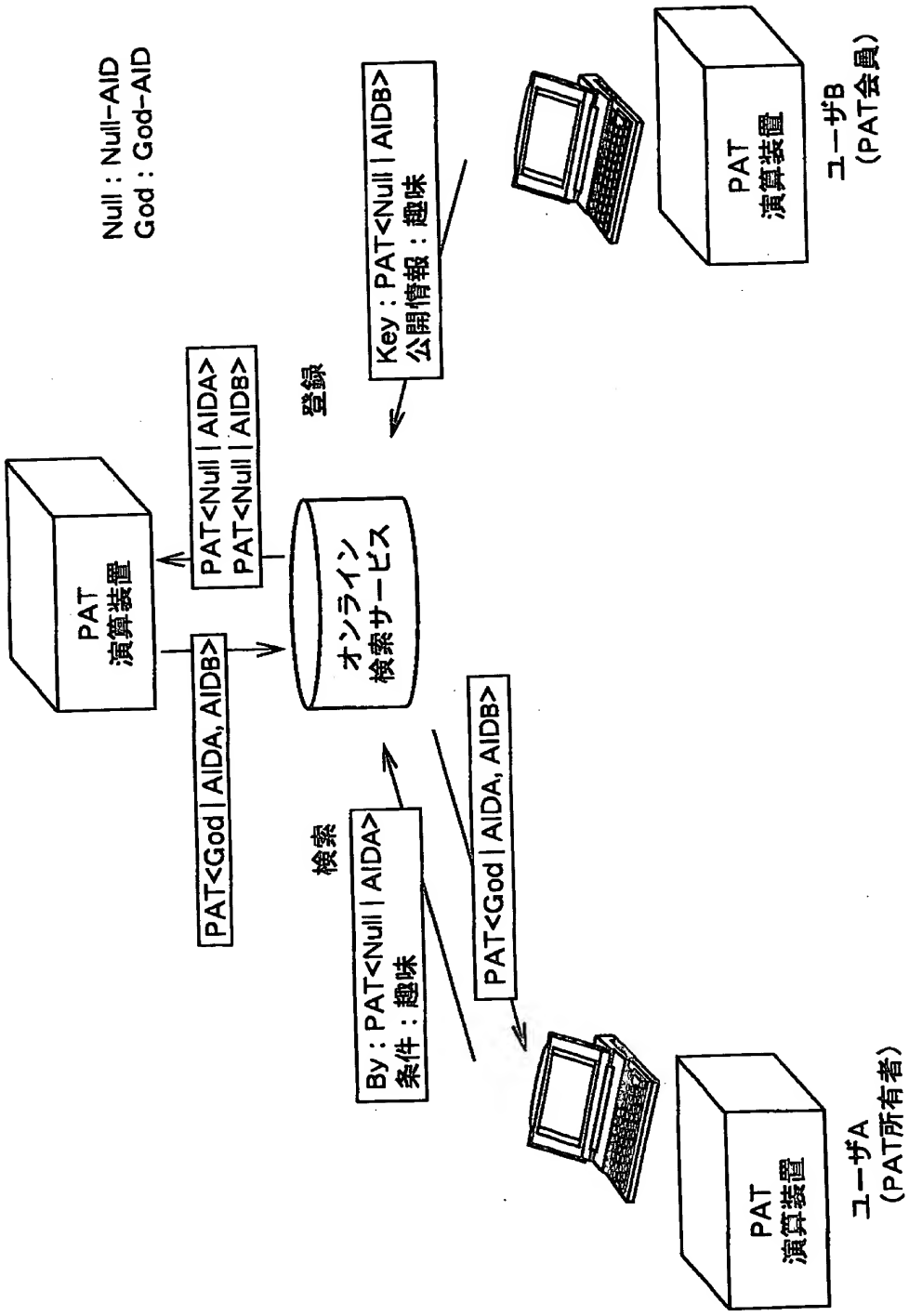
【図６６】


God-AID規則の処理
S6611
PAT所有者AIDとNull-AIDとGod-AIDを入力する
6613
所有者AIDとGod-AIDを文字比較する
S6615
完全に一致するか？
YES
NO
S6617
所有者AIDとNull-AIDを文字比較する
S6619
完全に一致するか？
YES
NO
S6621
Enabler of Null-AIDを入力する
S6623
Enablerの正当性を判定する
S6624
正当か？
NO
S6625
所有者AIDをGod-AIDで上書きする
S6627
Enabler of 所有者AIDを入力する
S6629
Enablerの正当性を判定する
S6631
正当か？
NO
YES
S6633
God-AIDをPATに連結する
S6635
所有者IndexをGod-AIDに設定する
処理中止(Abort)
終了
処理中止(Abort)

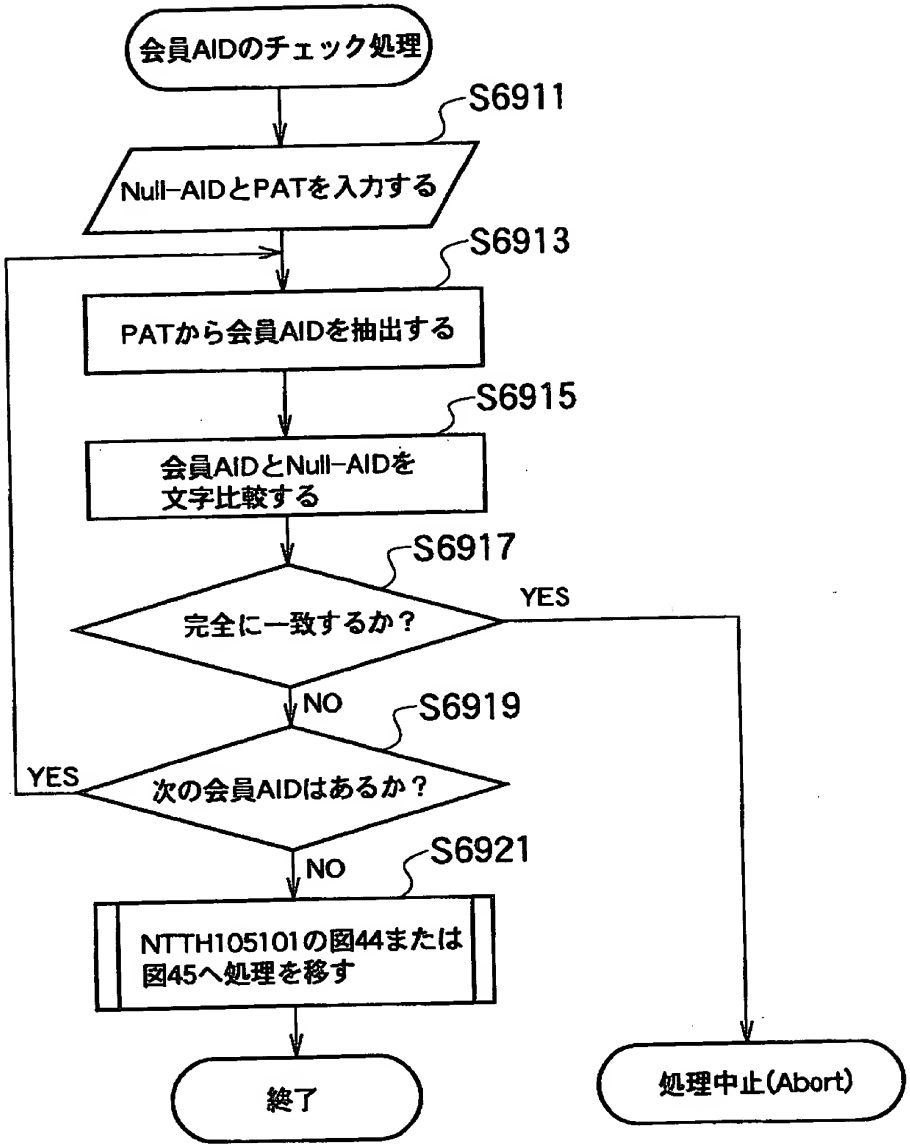
【図６７】


Null : Null-AID
God : God-AID
PAT
演算装置
PAT<Null | AIDA, AIDB>
PAT<God | AIDA, AIDB>
ユーザA
(PAT所有者)

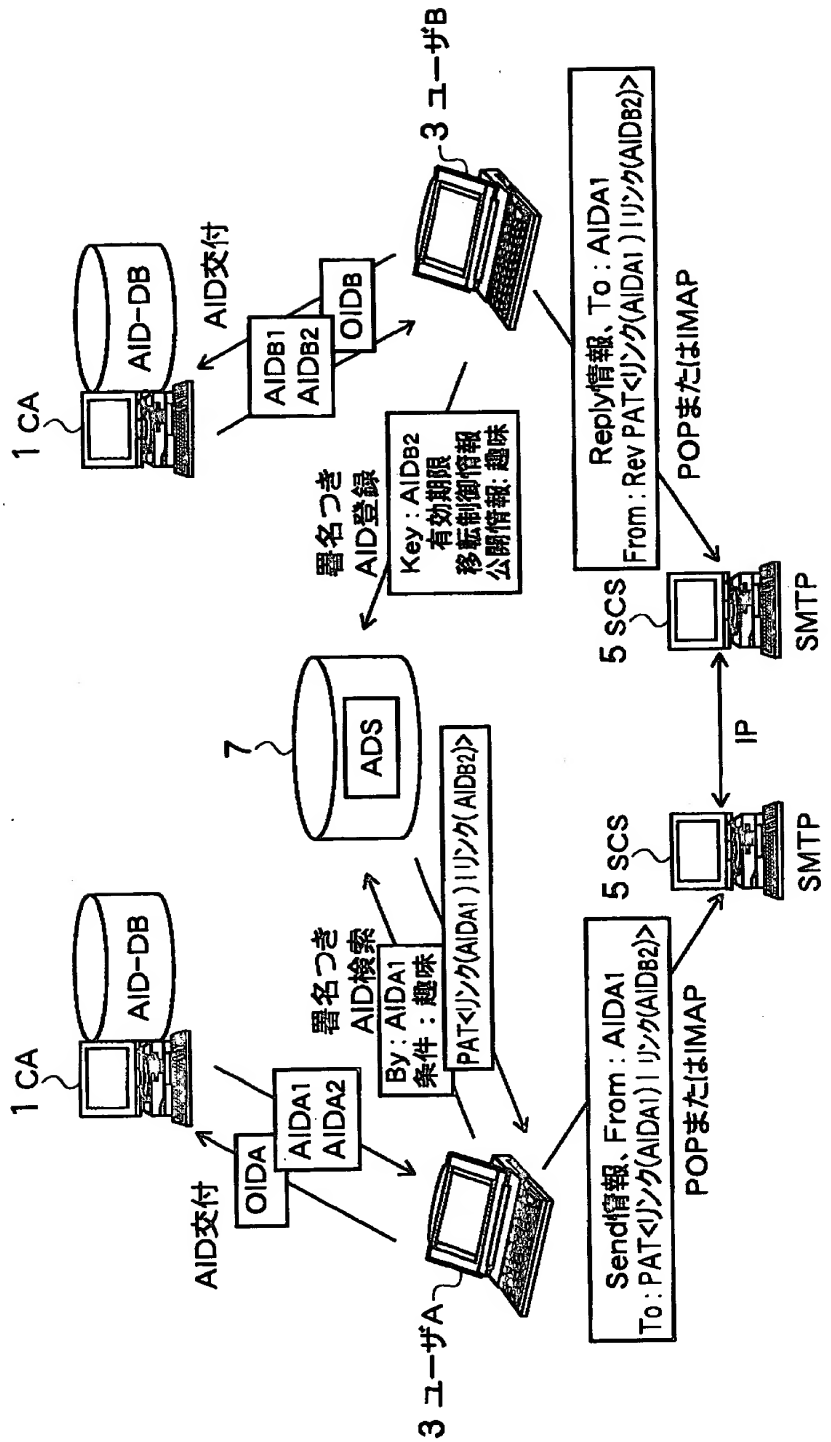
【図６８】


Null : Null-AID
God : God-AID
Key : PAT<Null | AIDB>
公開情報 : 趣味
PAT
演算装置
ユーザB
(PAT会員)
登録
PAT<Null | AIDA>
PAT<Null | AIDB>
PAT
演算装置
オンライン
検索サービス
PAT<God | AIDA, AIDB>
検索
By : PAT<Null | AIDA>
条件 : 趣味
PAT<God | AIDA, AIDB>
PAT
演算装置
ユーザA
(PAT所有者)

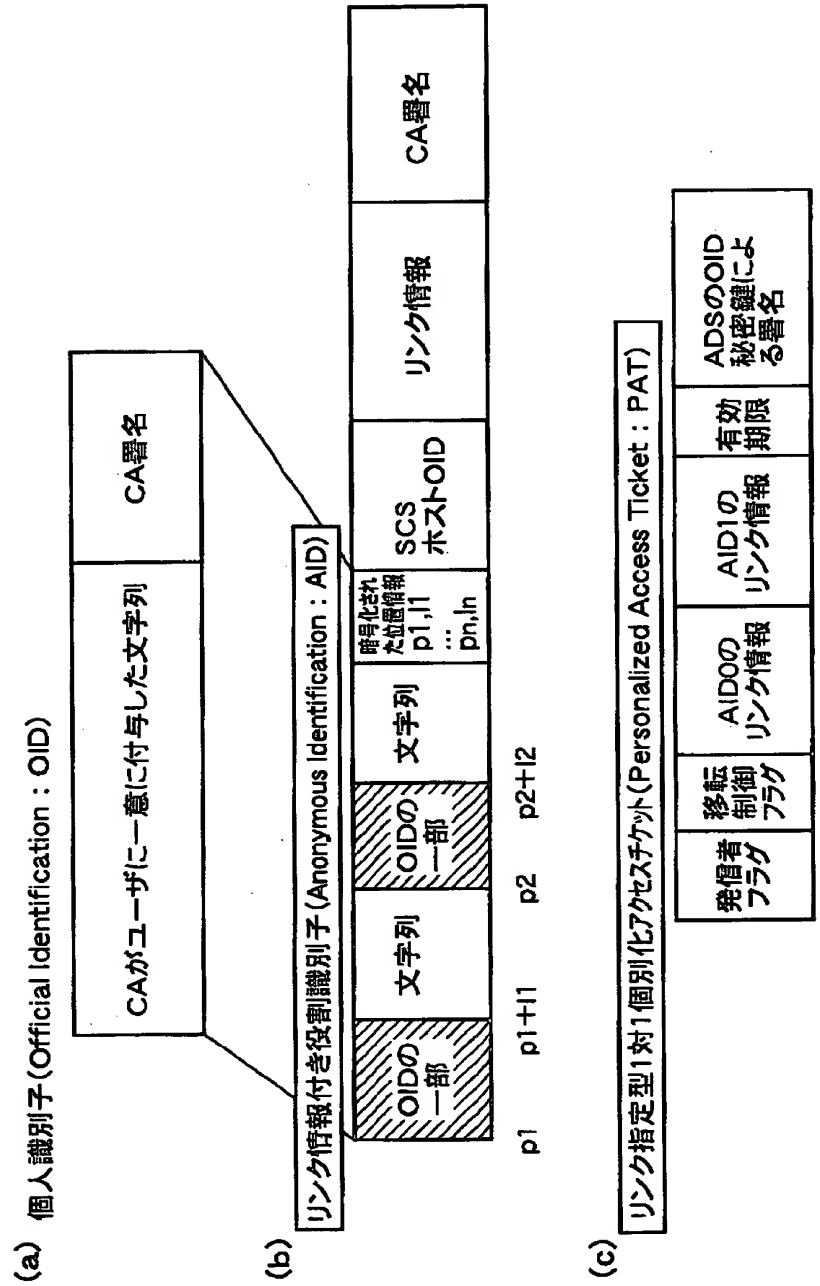
【図６９】


会員AIDのチェック処理
S6911
Null-AIDとPATを入力する
S6913
PATから会員AIDを抽出する
S6915
会員AIDとNull-AIDを
文字比較する
S6917
完全に一致するか？
YES
NO
S6919
次の会員AIDはあるか？
YES
NO
S6921
NTTH105101の図44または
図45へ処理を移す
終了
処理中止(Abort)

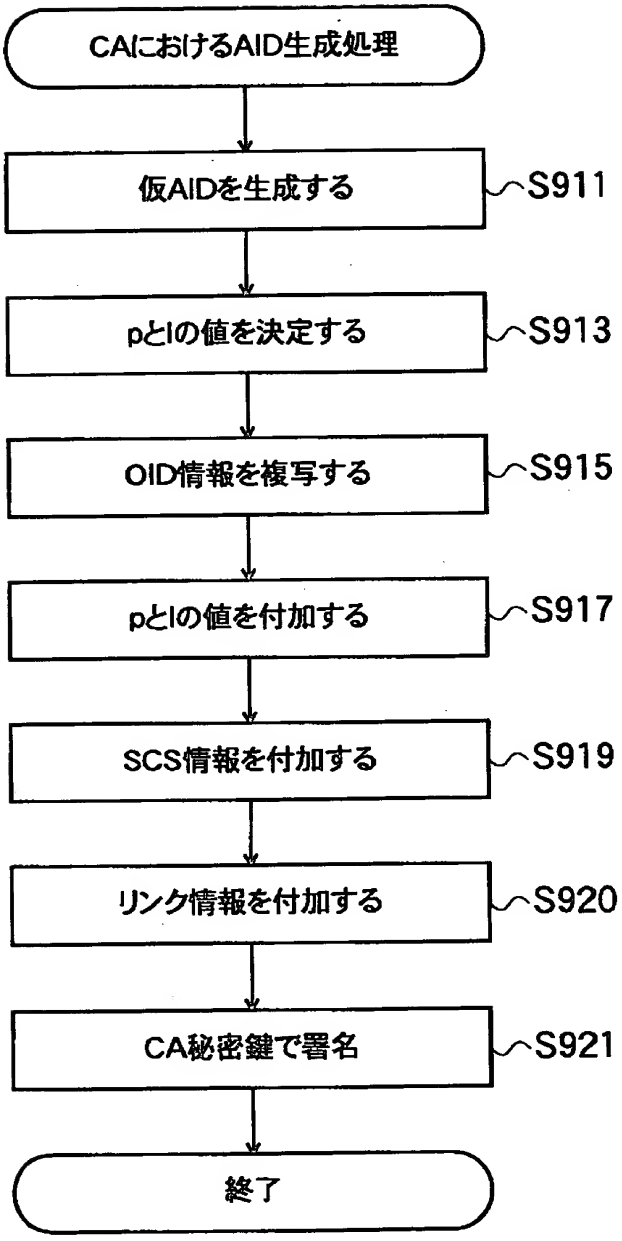
【図７０】


1 CA
AID-DB
AID交付
AIDB1
AIDB2
OIDB
3 ユーザB
署名つき
AID登録
Key : AIDB2
有効期限
移転制御情報
公開情報: 趣味
Reply情報、To : AIDA1
From : Rev PAT<リンク(AIDA1)>リンク(AIDB2)>
POPまたはIMAP
5 SCS
SMTP
IP
7
ADS
PAT<リンク(AIDA1)>リンク(AIDB2)>
署名つき
AID検索
By : AIDA1
条件 : 趣味
1 CA
AID-DB
OIDA
AIDA1
AIDA2
AID交付
3 ユーザA
Send情報、From : AIDA1
To : PAT<リンク(AIDA1)>リンク(AIDB2)>
POPまたはIMAP
5 SCS
SMTP

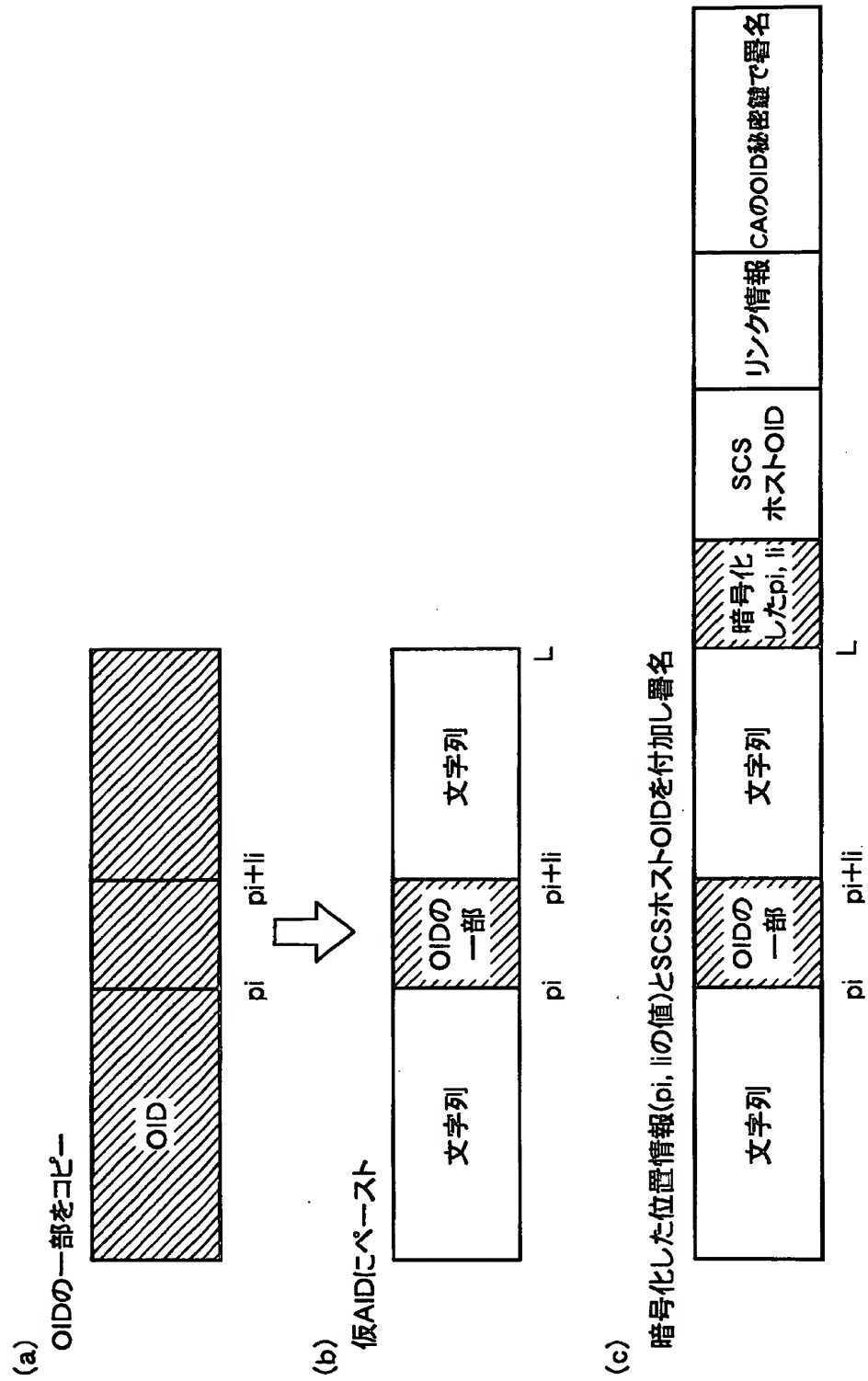
【図７１】


(a) 個人識別子(Official Identification : OID)
CAがユーザに一意に付与した文字列
CA署名
(b)
リンク情報付き役割識別子(Anonymous Identification : AID)
OIDの一部
文字列
OIDの一部
文字列
暗号化された位置情報 p1,l1 … pn,ln
SCS ホストOID
リンク情報
CA署名
p1
p1+l1
p2
p2+l2
(c)
リンク指定型1対1個別化アクセスチケット(Personalized Access Ticket : PAT)
発信者フラグ
移転制御フラグ
AIDのリンク情報
AID1のリンク情報
有効期限
ADSのOID秘密鍵による署名

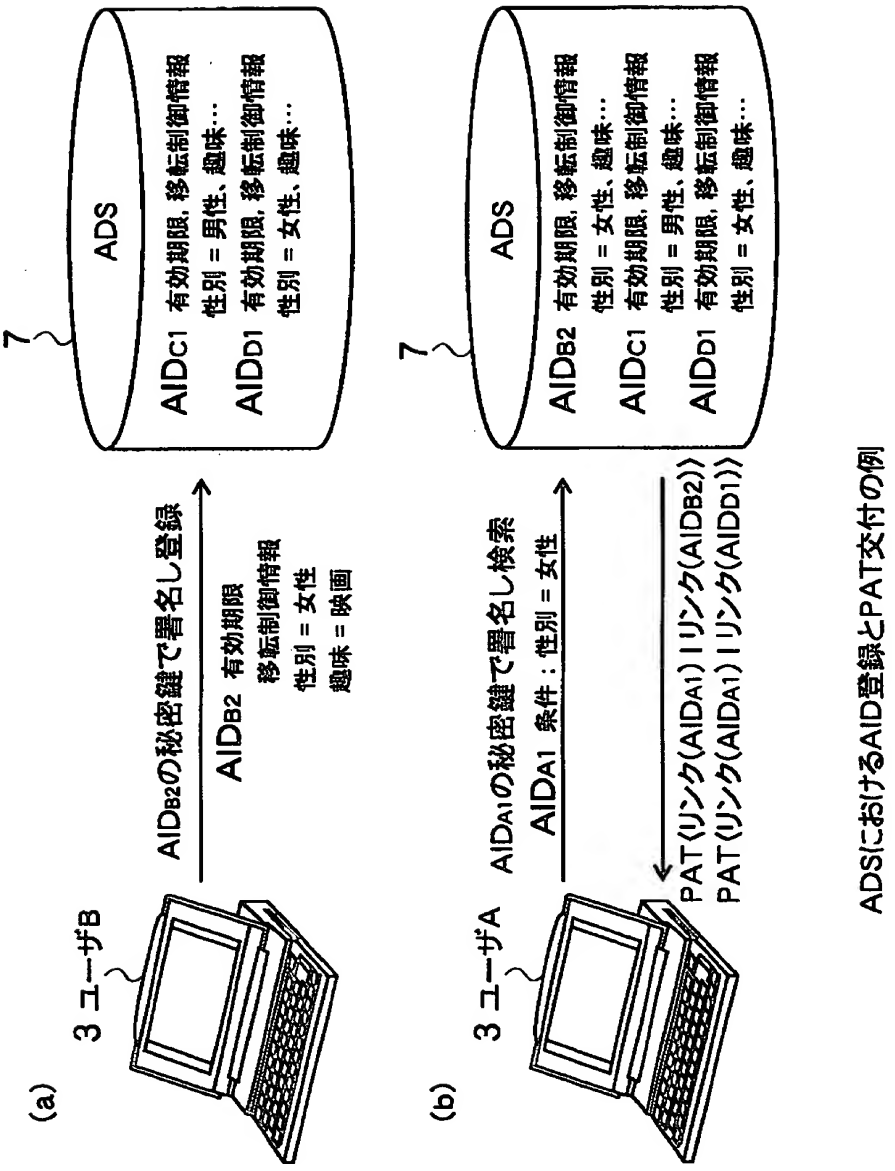
【図７２】


CAにおけるAID生成処理
仮AIDを生成する
S911
pとlの値を決定する
S913
OID情報を複写する
S915
pとlの値を付加する
S917
SCS情報を付加する
S919
リンク情報を付加する
S920
CA秘密鍵で署名
S921
終了

【図７３】

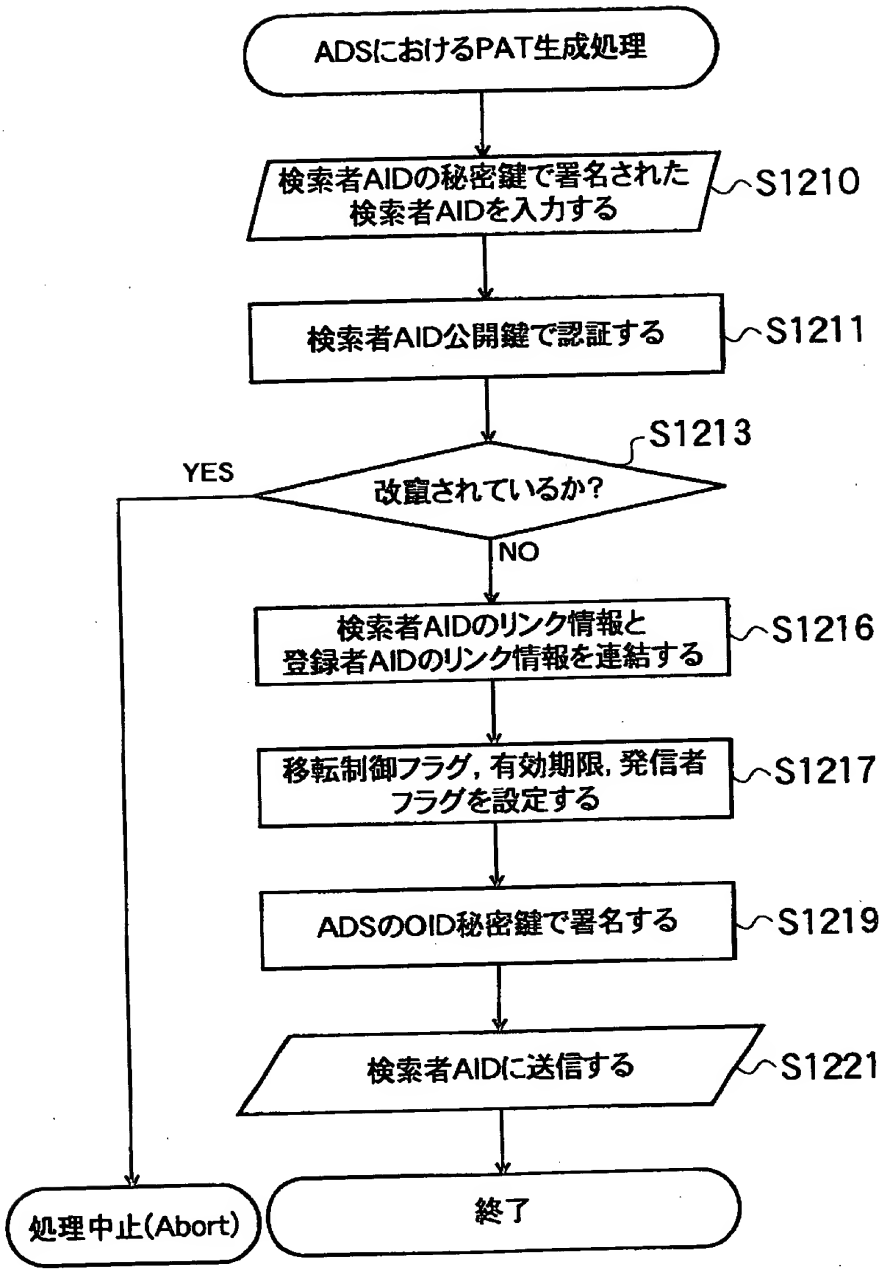

(a)
OIDの一部をコピー
OID
pi
pi+li
(b)
仮AIDにペースト
文字列
OIDの一部
文字列
pi
pi+li
L
(c)
暗号化した位置情報(pi, liの値)とSCSホストOIDを付加し署名
文字列
OIDの一部
文字列
暗号化したpi, li
SCSホストOID
リンク情報
CAのOID秘密鍵で署名
pi
pi+li
L

【図７４】

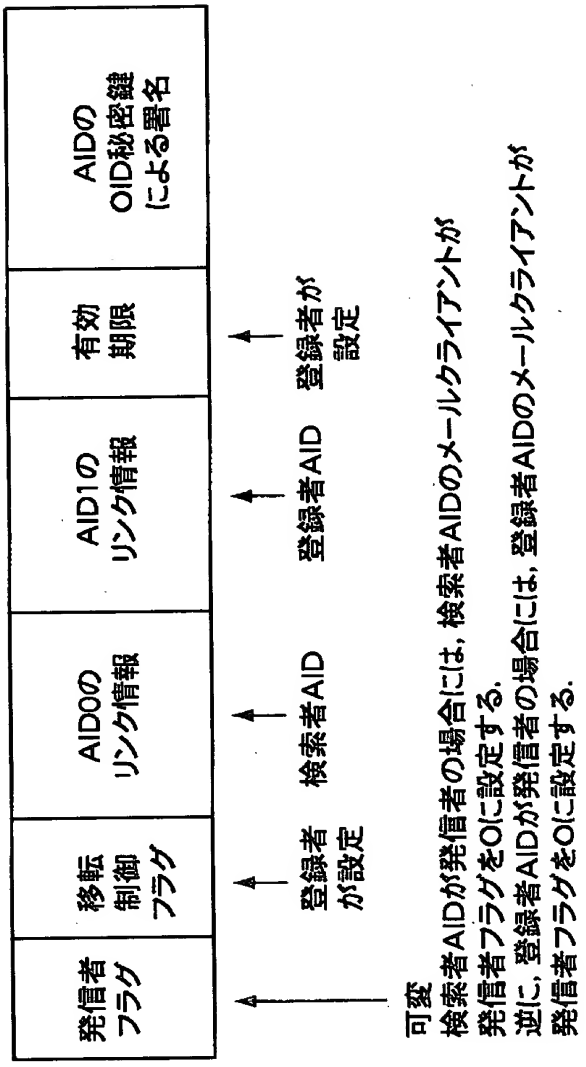


ADSにおけるAID登録とPAT交付の例

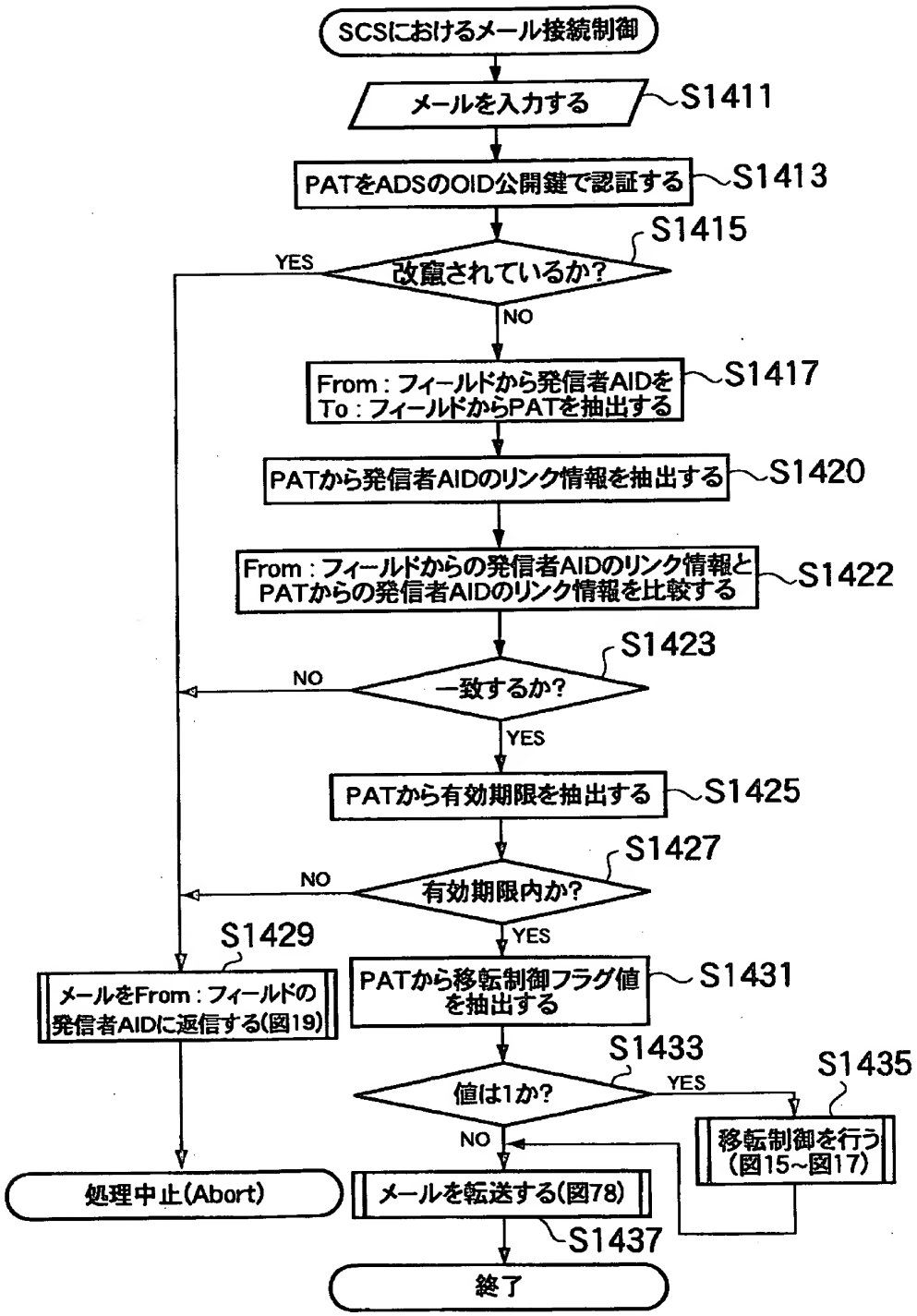
【図７５】


ADSにおけるPAT生成処理
検索者AIDの秘密鍵で署名された検索者AIDを入力する
S1210
検索者AID公開鍵で認証する
S1211
S1213
改竄されているか?
YES
NO
検索者AIDのリンク情報と登録者AIDのリンク情報を連結する
S1216
移転制御フラグ, 有効期限, 発信者フラグを設定する
S1217
ADSのOID秘密鍵で署名する
S1219
検索者AIDに送信する
S1221
処理中止(Abort)
終了

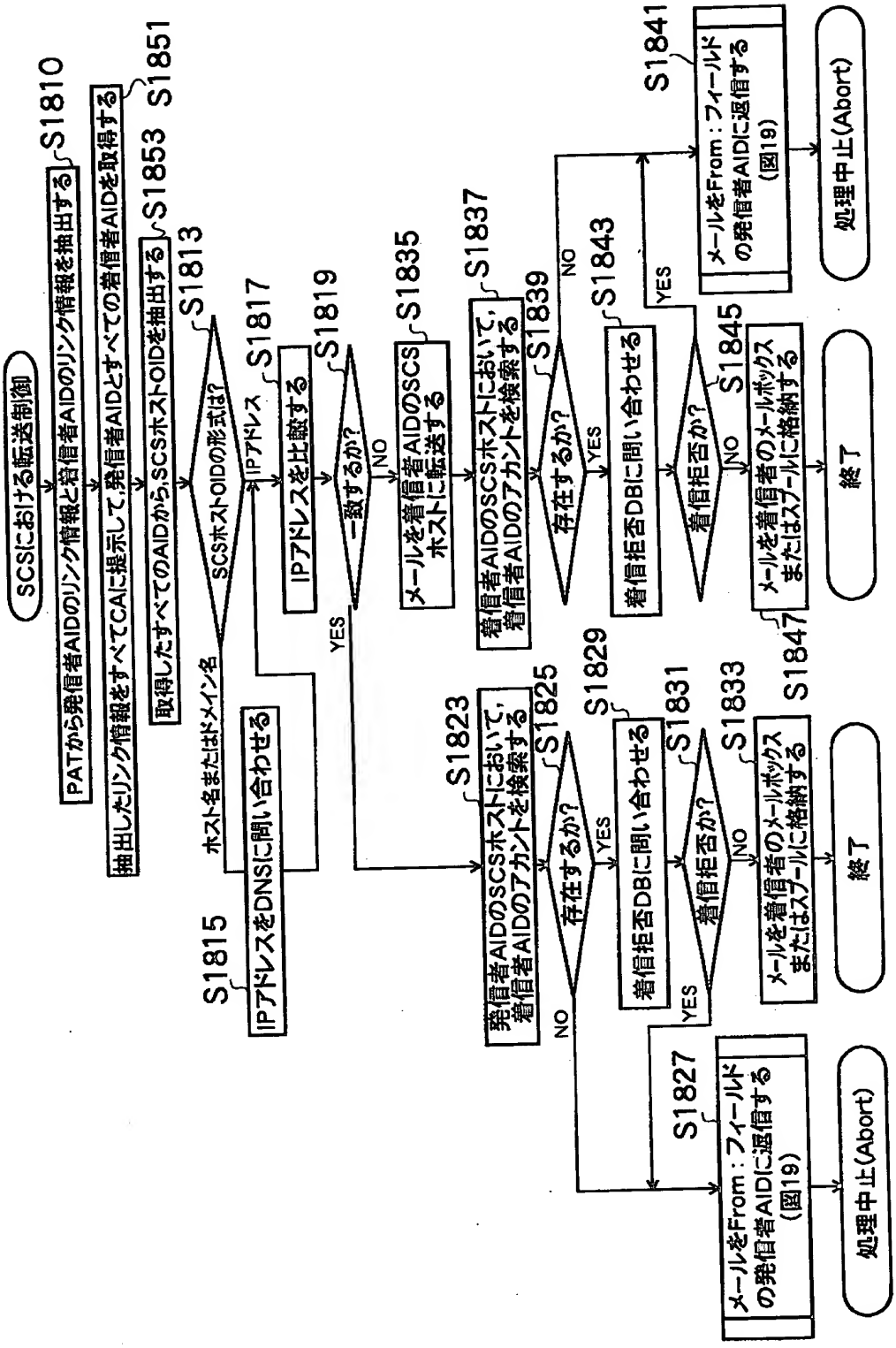
【図７６】


発信者フラグ
移転制御フラグ
AIDOのリンク情報
AID1のリンク情報
有効期限
AIDのOID秘密鍵による署名
登録者が設定
検索者AID
登録者AID
登録者が設定
可変
検索者AIDが発信者の場合には，検索者AIDのメールクライアントが
発信者フラグを0に設定する．
逆に，登録者AIDが発信者の場合には，登録者AIDのメールクライアントが
発信者フラグを0に設定する．

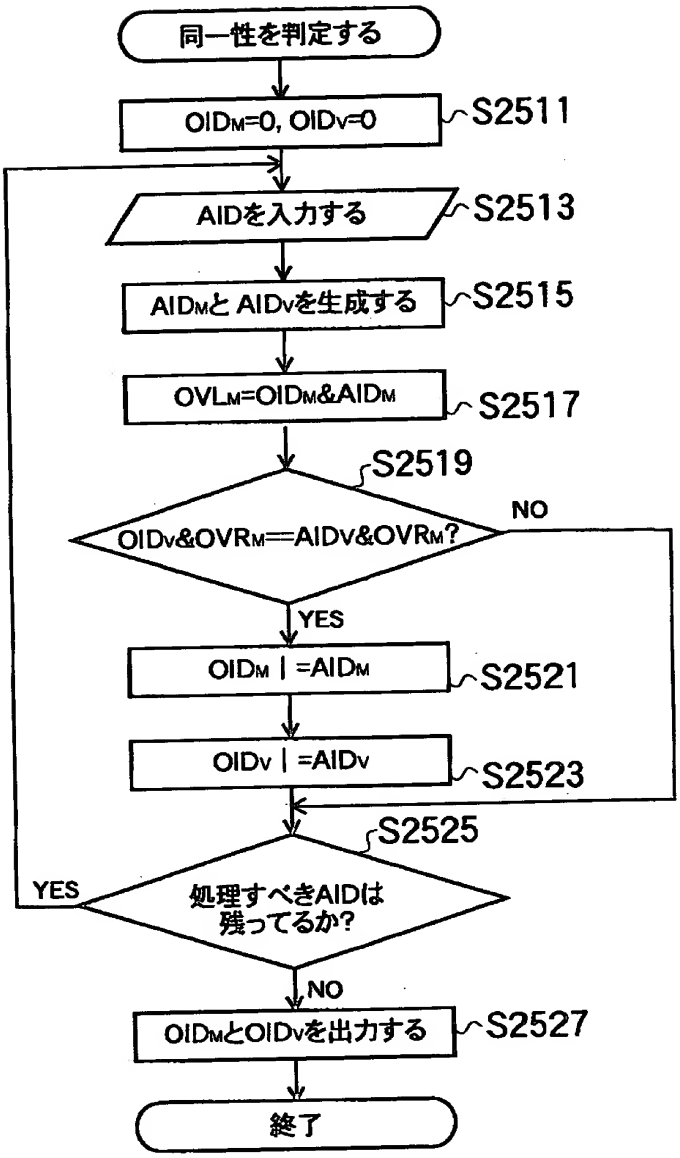
【図７７】


SCSにおけるメール接続制御
メールを入力する
S1411
PATをADSのOID公開鍵で認証する
S1413
S1415
改竄されているか?
YES
NO
From：フィールドから発信者AIDを
To：フィールドからPATを抽出する
S1417
PATから発信者AIDのリンク情報を抽出する
S1420
From：フィールドからの発信者AIDのリンク情報と
PATからの発信者AIDのリンク情報を比較する
S1422
S1423
一致するか?
NO
YES
PATから有効期限を抽出する
S1425
S1427
有効期限内か?
NO
YES
S1429
メールをFrom：フィールドの
発信者AIDに返信する(図19)
PATから移転制御フラグ値
を抽出する
S1431
S1433
値は1か?
YES
S1435
移転制御を行う
(図15~図17)
NO
処理中止(Abort)
メールを転送する(図78)
S1437
終了

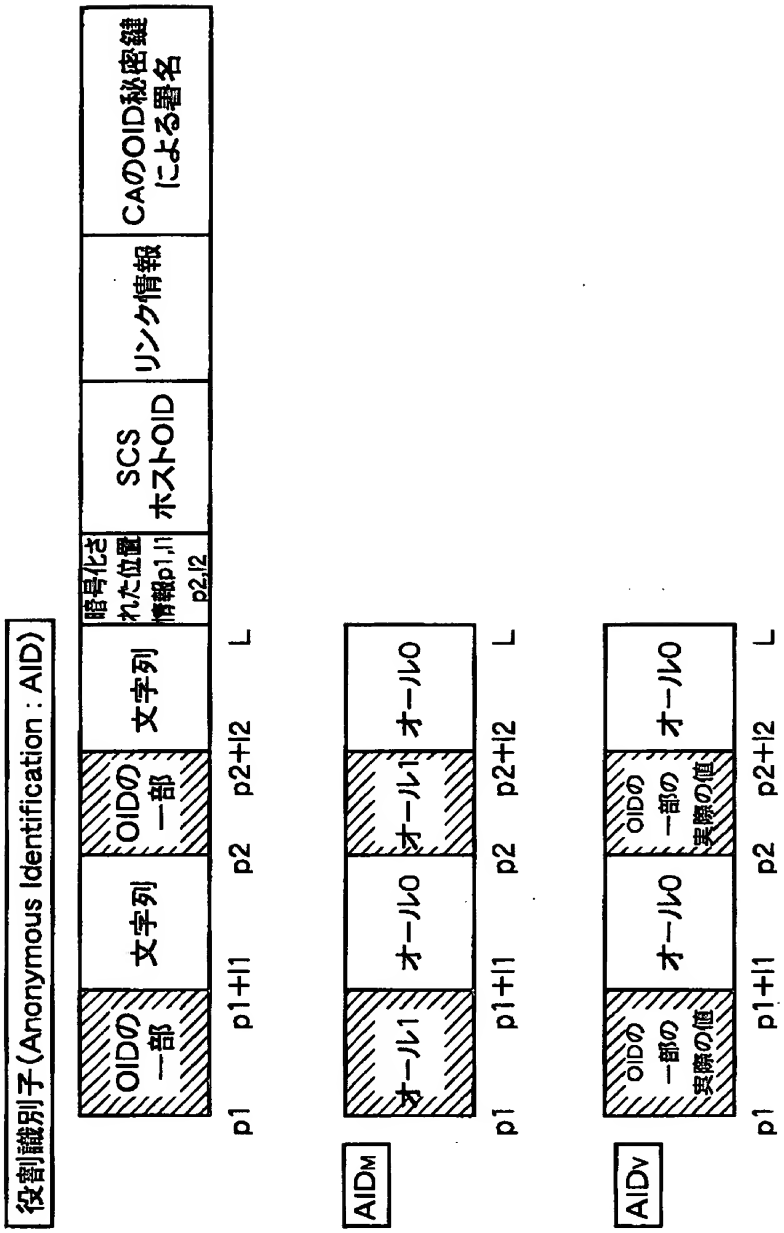
【図７８】


SCSにおける転送制御
S1810
PATから発信者AIDのリンク情報と着信者AIDのリンク情報を抽出する
S1851
抽出したリンク情報をすべてCAに提示して,発信者AIDとすべての着信者AIDを取得する
S1853
取得したすべてのAIDから,SCSホストOIDを抽出する
S1813
SCSホストOIDの形式は?
ホスト名またはドメイン名
S1815
IPアドレスをDNSに問い合わせる
IPアドレス
S1817
IPアドレスを比較する
S1819
一致するか?
YES
NO
S1835
メールを着信者AIDのSCSホストに転送する
S1823
発信者AIDのSCSホストにおいて,着信者AIDのアカントを検索する
S1837
着信者AIDのSCSホストにおいて,着信者AIDのアカントを検索する
S1825
存在するか?
YES
NO
S1829
着信拒否DBに問い合わせる
S1839
存在するか?
YES
NO
S1843
着信拒否DBに問い合わせる
S1831
着信拒否か?
YES
NO
S1833
メールを着信者のメールボックスまたはスプールに格納する
S1847
着信拒否か?
YES
NO
S1845
メールを着信者のメールボックスまたはスプールに格納する
S1827
メールをFrom:フィールドの発信者AIDに返信する(図19)
S1841
メールをFrom:フィールドの発信者AIDに返信する(図19)
終了
終了
処理中止(Abort)
処理中止(Abort)

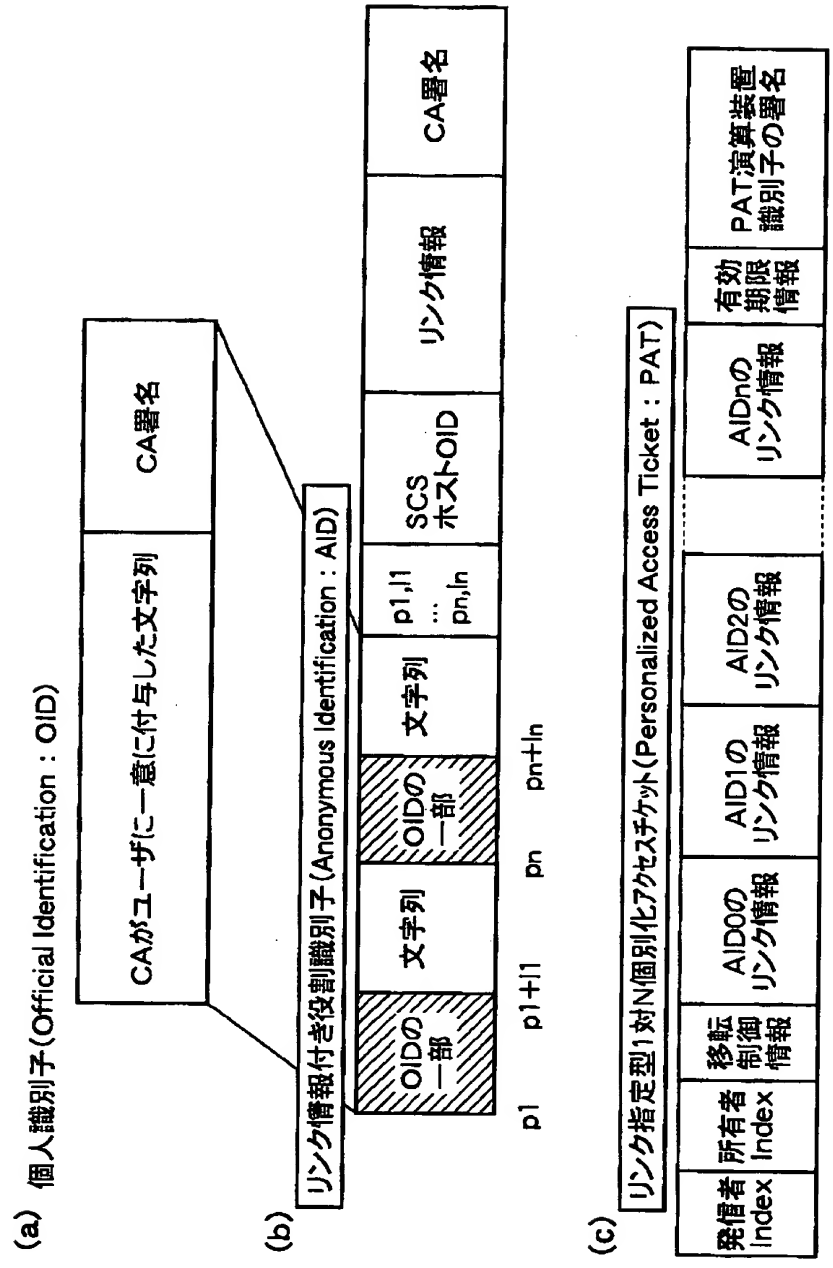
【図７９】


同一性を判定する
OIDM=0, OIDV=0
S2511
AIDを入力する
S2513
AIDMとAIDVを生成する
S2515
OVLM=OIDM&AIDM
S2517
S2519
OIDV&OVRM==AIDV&OVRM?
NO
YES
OIDM | =AIDM
S2521
OIDV | =AIDV
S2523
S2525
YES
処理すべきAIDは
残ってるか?
NO
OIDMとOIDVを出力する
S2527
終了

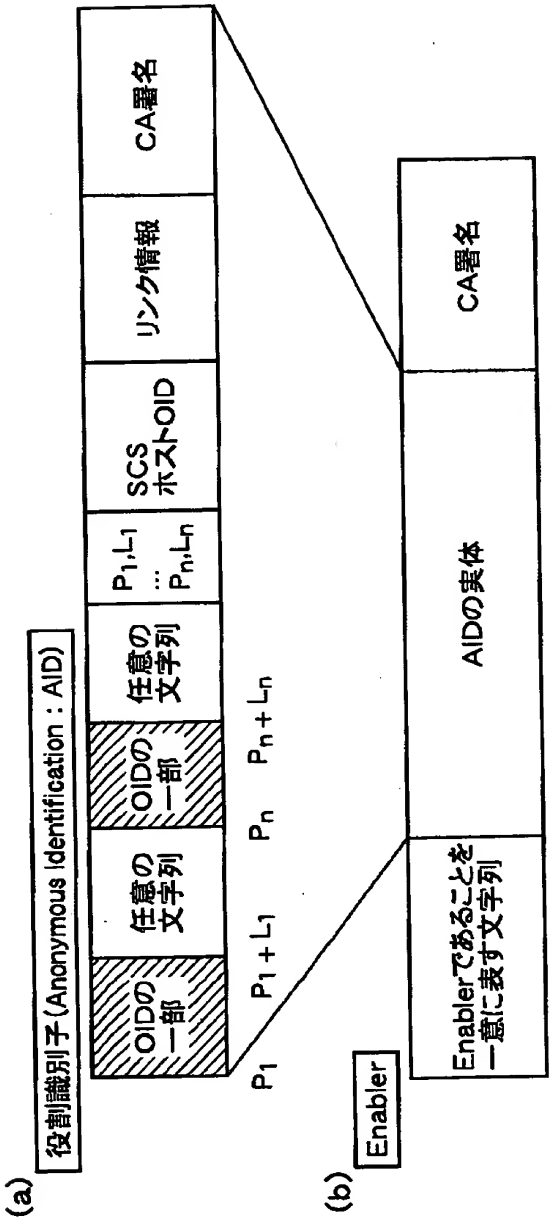
【図８０】


役割識別子(Anonymous Identification : AID)
OIDの一部
文字列
OIDの一部
文字列
暗号化された位置情報p1,l1 p2,l2
SCSホストOID
リンク情報
CAのOID秘密鍵による署名
p1
p1+l1
p2
p2+l2
L
AIDM
オール1
オール0
オール1
オール0
AIDV
OIDの一部の実際の値
オール0
OIDの一部の実際の値
オール0

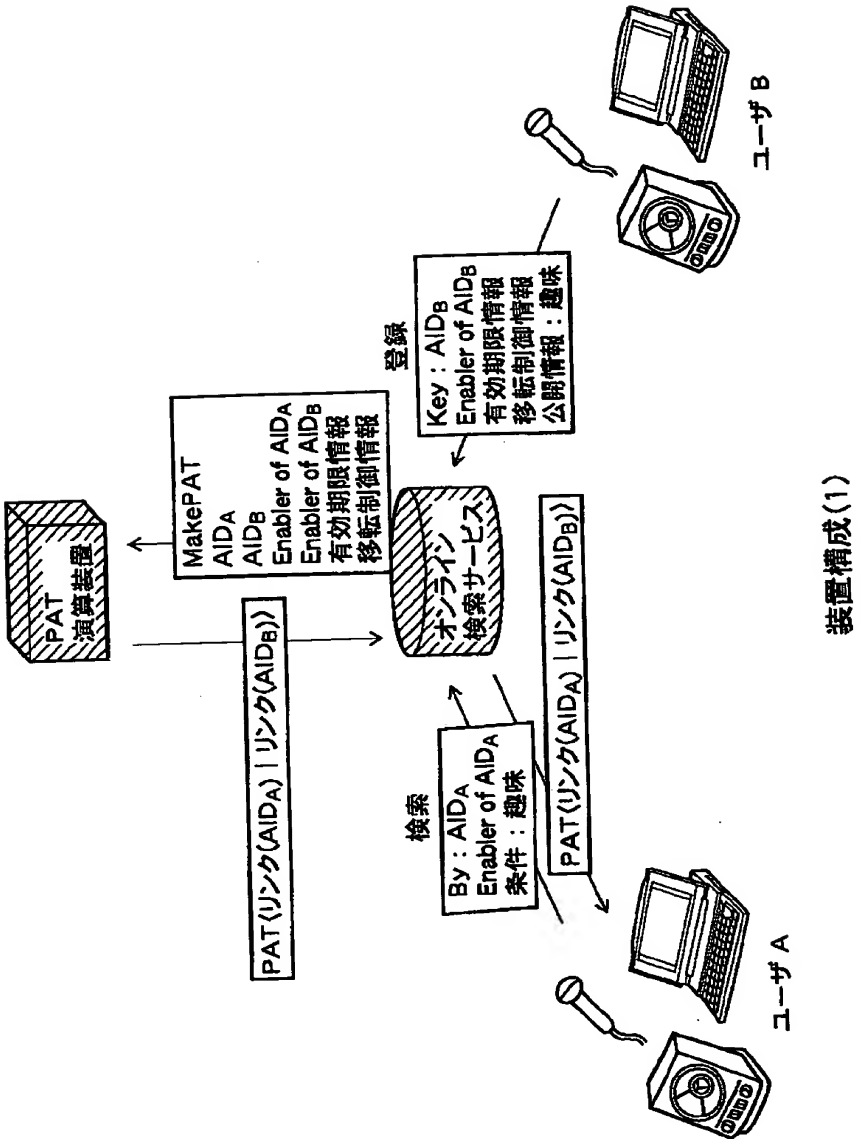
【図８１】


(a) 個人識別子(Official Identification : OID)
CAがユーザに一意に付与した文字列
CA署名
(b)
リンク情報付き役割識別子(Anonymous Identification : AID)
OIDの一部
文字列
OIDの一部
文字列
p1,l1
...
pn,ln
SCS ホストOID
リンク情報
CA署名
p1
p1+l1
pn
pn+ln
(c)
リンク指定型1対N個別化アクセスチケット(Personalized Access Ticket : PAT)
発信者 Index
所有者 Index
移転制御情報
AID0のリンク情報
AID1のリンク情報
AID2のリンク情報
AIDnのリンク情報
有効期限情報
PAT:演算装置識別子の署名

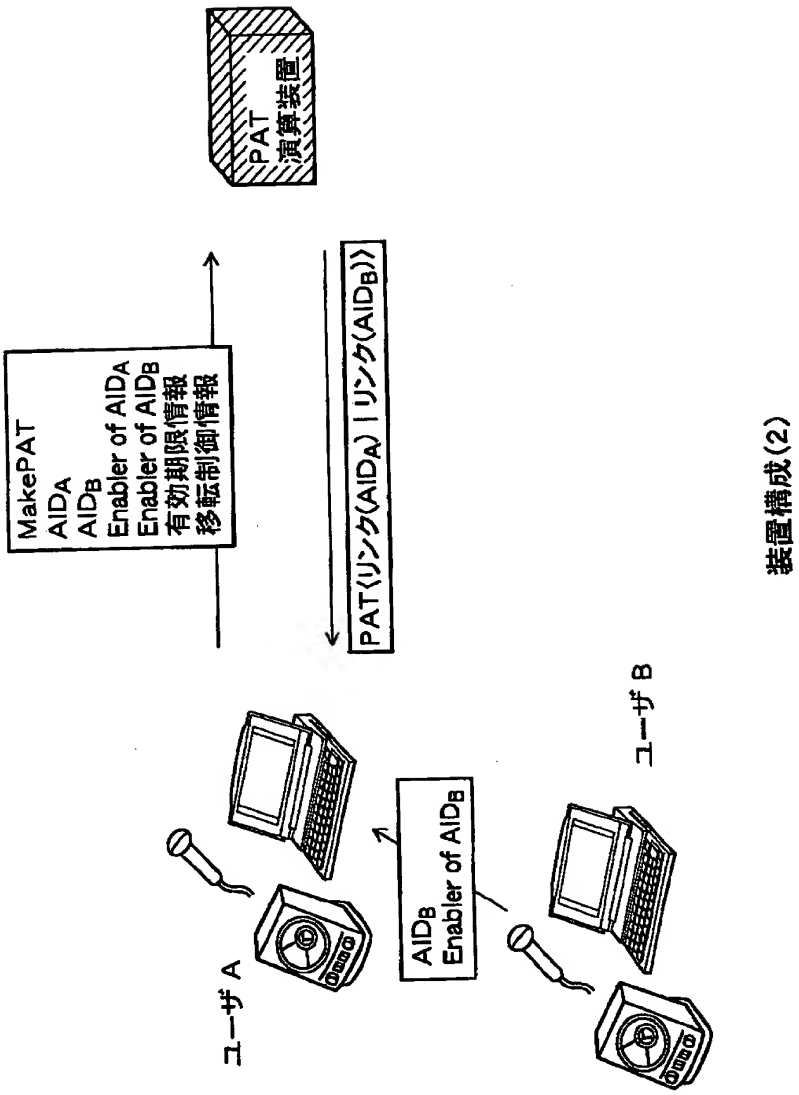
【図８２】


(a)
役割識別子(Anonymous Identification : AID)
OIDの一部
任意の文字列
OIDの一部
任意の文字列
P1,L1 … Pn,Ln
SCSホストOID
リンク情報
CA署名
P1
P1 + L1
Pn
Pn + Ln
(b)
Enabler
Enablerであることを一意に表す文字列
AIDの実体
CA署名

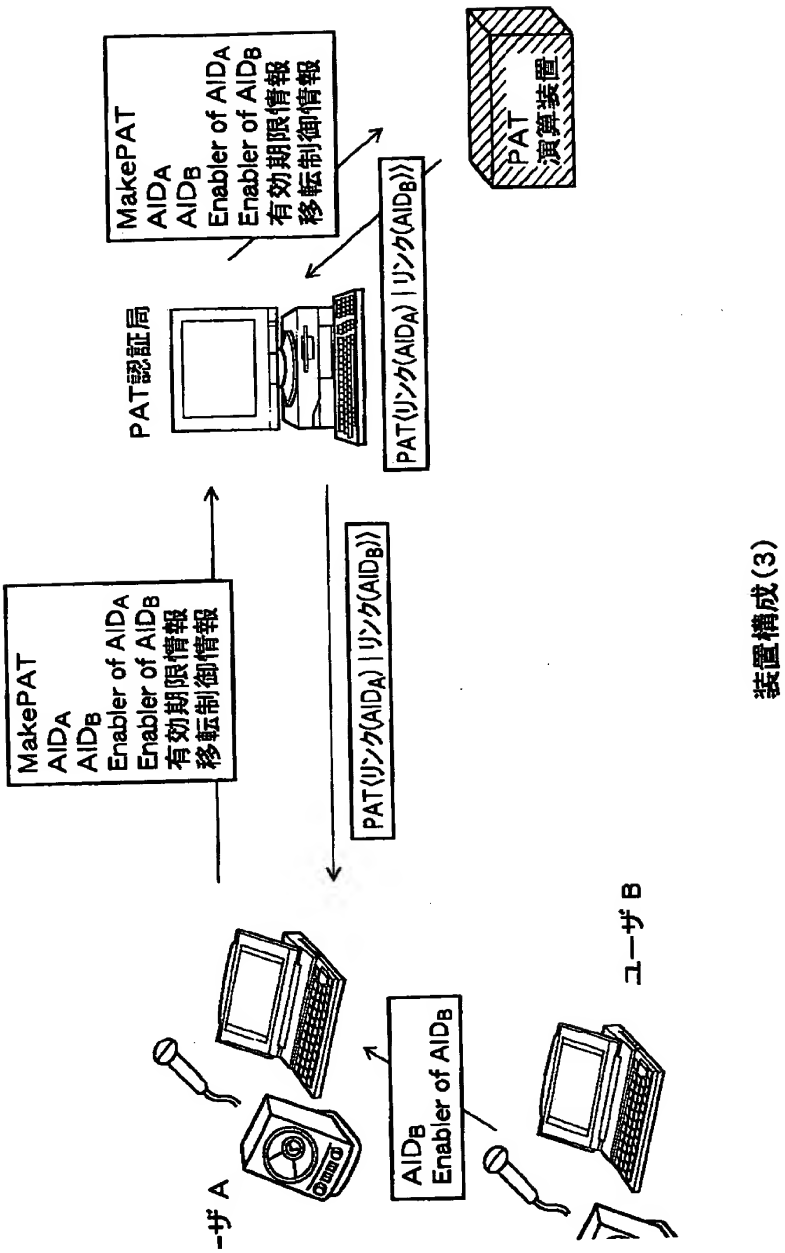
【図８３】


PAT
演算装置
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
オンライン
検索サービス
登録
Key：AIDB
Enabler of AIDB
有効期限情報
移転制御情報
公開情報：趣味
ユーザB
PAT〈リンク(AIDA)｜リンク(AIDB)〉
検索
By：AIDA
Enabler of AIDA
条件：趣味
PAT〈リンク(AIDA)｜リンク(AIDB)〉
ユーザA
装置構成(1)

【図８４】

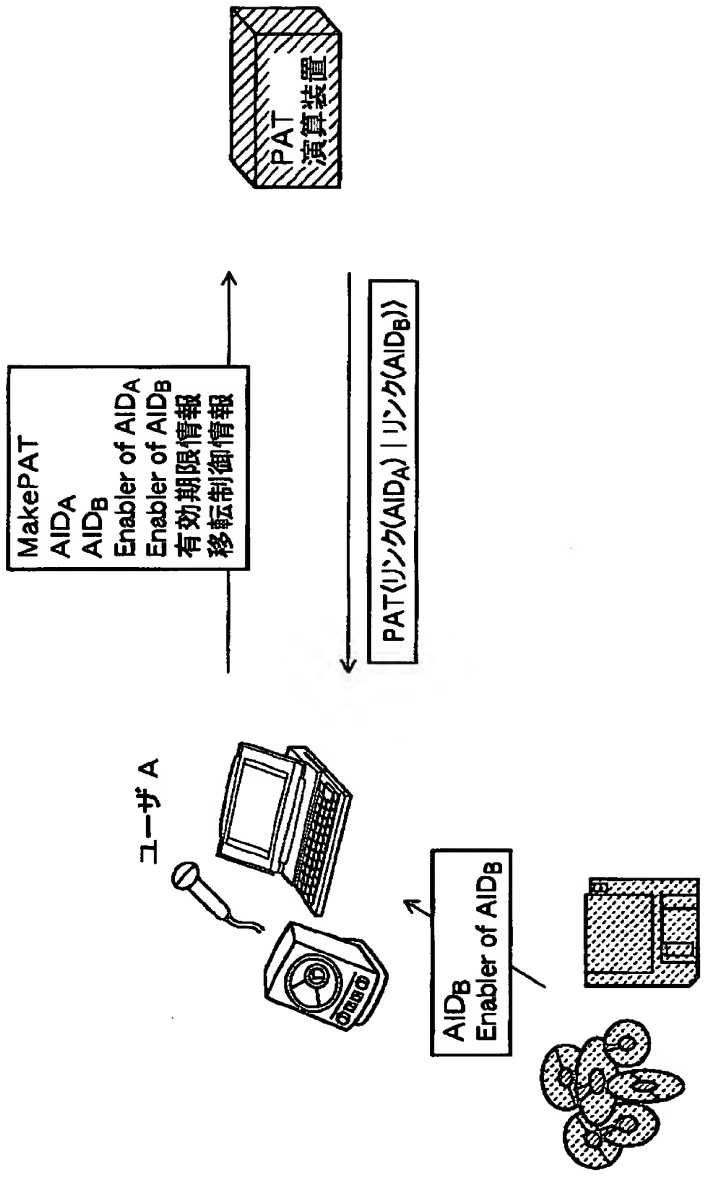

PAT
演算装置
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT〈リンク(AIDA)｜リンク(AIDB)〉
ユーザA
AIDB
Enabler of AIDB
ユーザB
装置構成(2)

【図８５】


MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT
演算装置
PAT認証局
PAT〈リンク(AIDA)|リンク(AIDB)〉
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT〈リンク(AIDA)|リンク(AIDB)〉
AIDB
Enabler of AIDB
ユーザ B
ーザ A

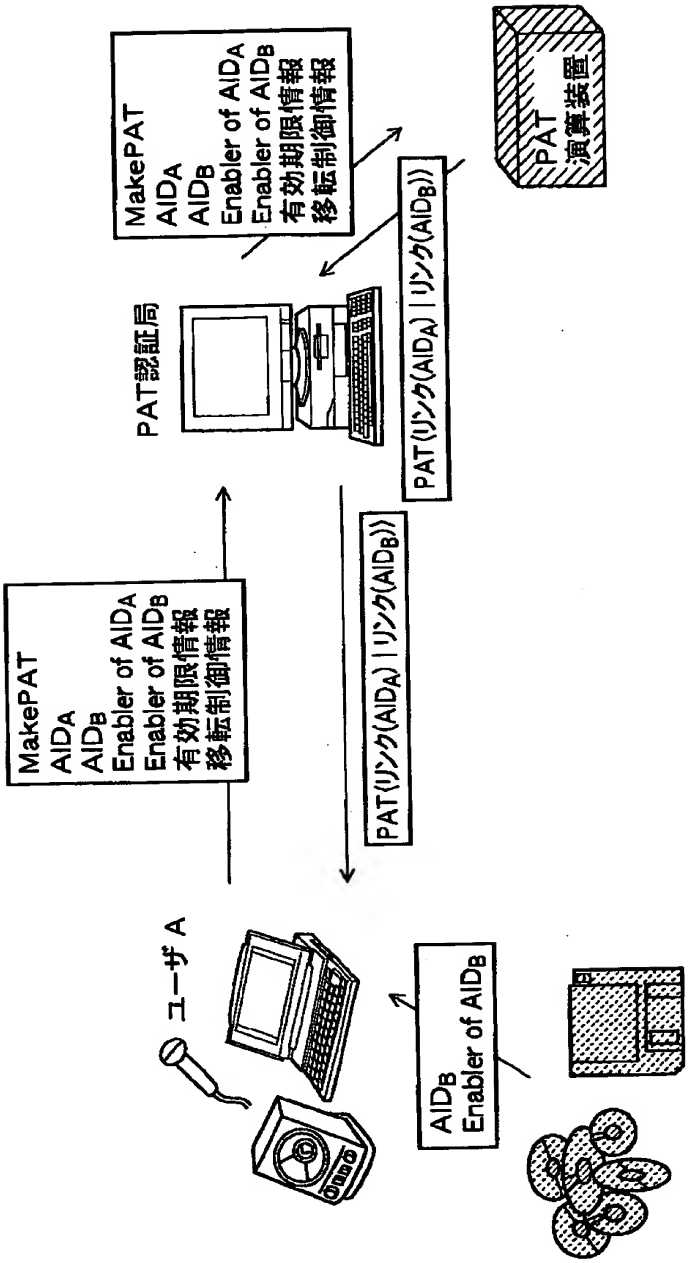
装置構成(3)

【図８６】


PAT
演算装置
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT(リンク(AIDA)|リンク(AIDB))
ユーザA
AIDB
Enabler of AIDB

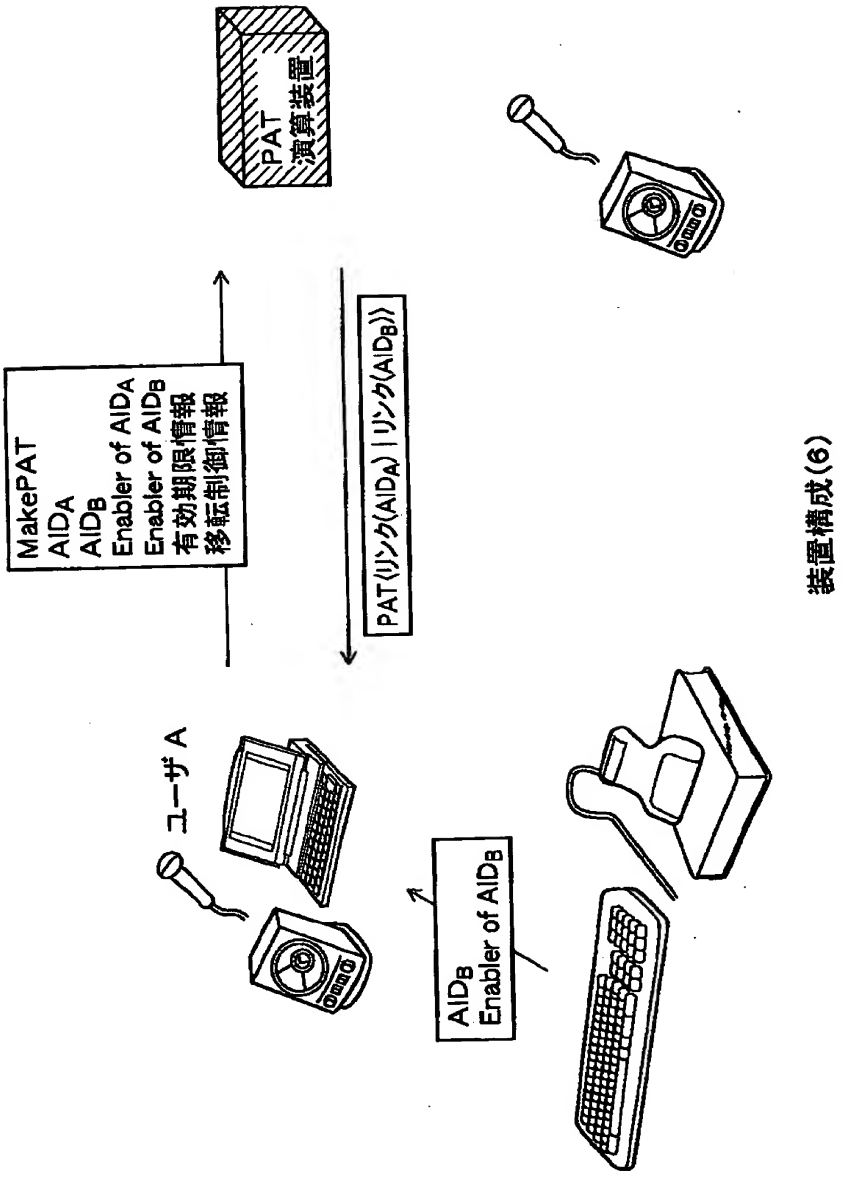
装置構成(4)

【図８７】

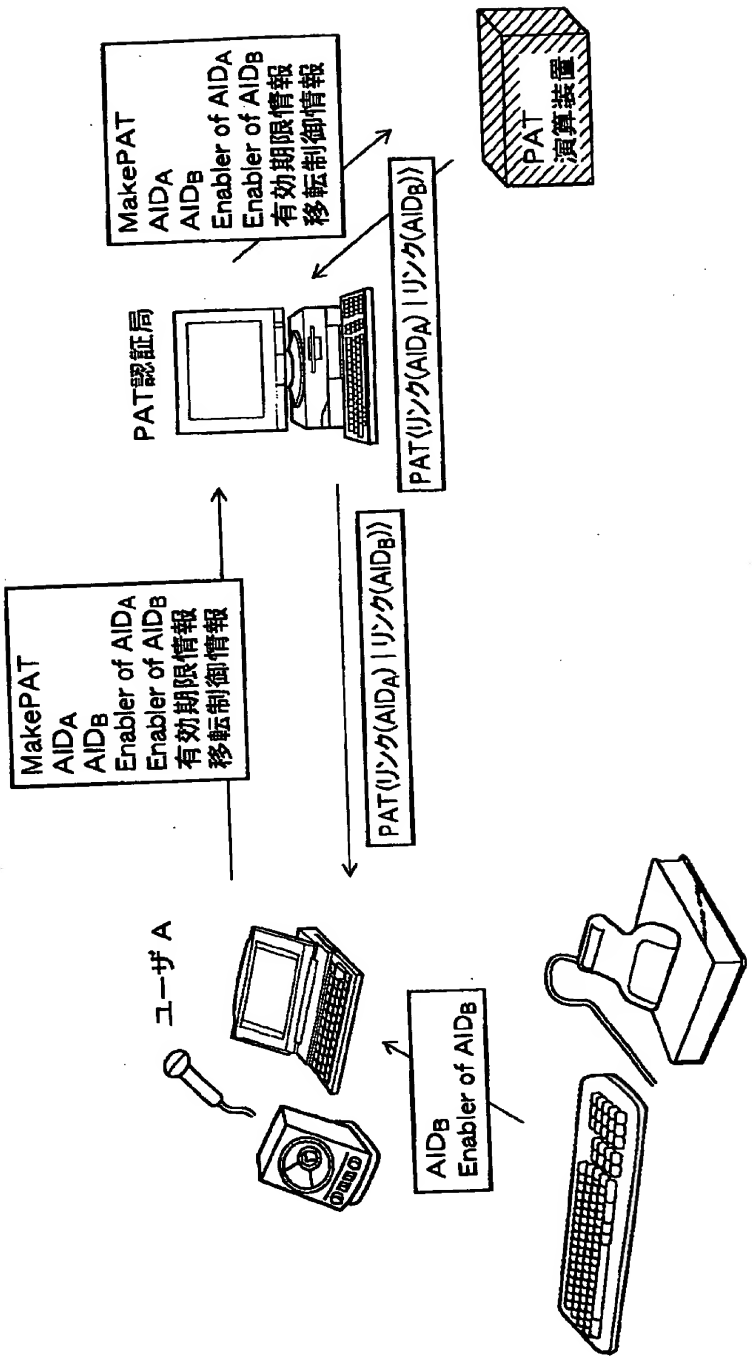

MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT
演算装置
PAT認証局
PAT(リンク(AIDA)|リンク(AIDB))
PAT(リンク(AIDA)|リンク(AIDB))
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
ユーザA
AIDB
Enabler of AIDB

装置構成(5)

【図８８】

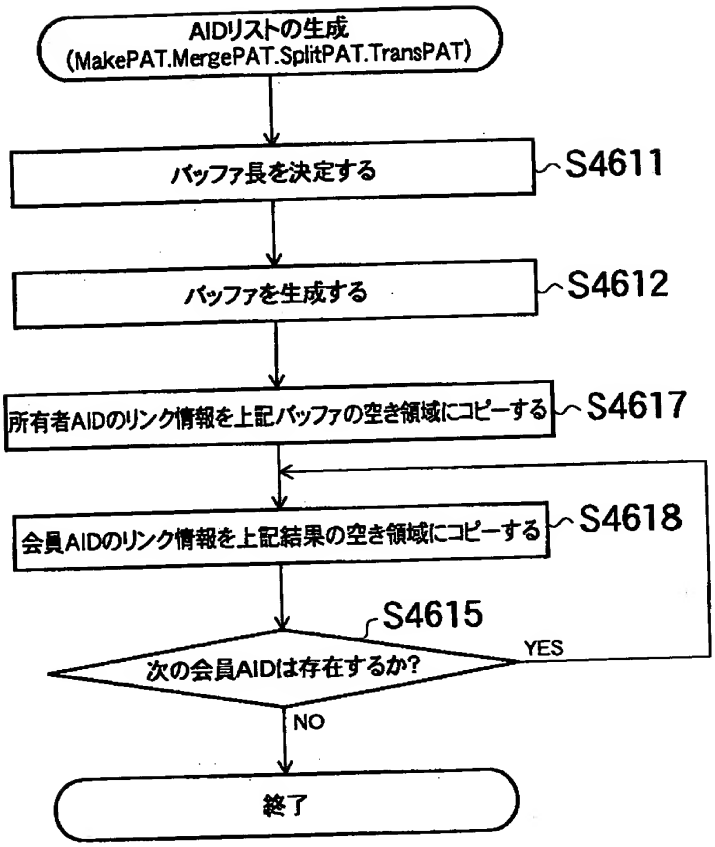

PAT
演算装置
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT〈リンク〈AIDA〉|リンク〈AIDB〉〉
ユーザA
AIDB
Enabler of AIDB
装置構成(6)

【図８９】

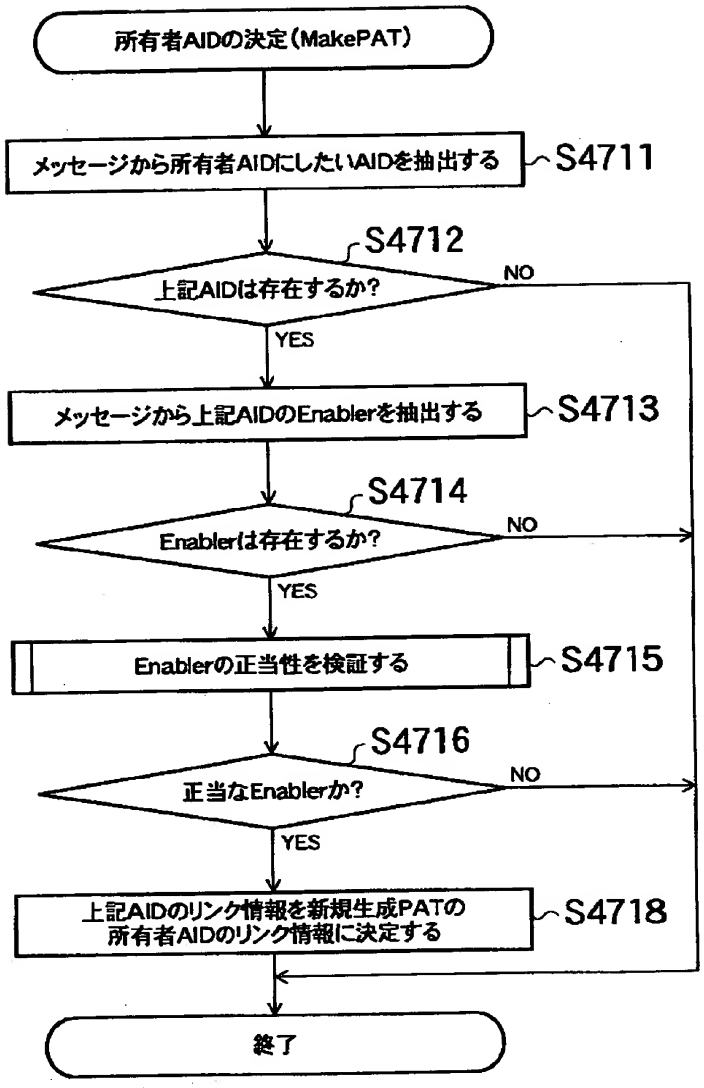

MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
PAT
演算装置
PAT認証局
PAT(リンク(AIDA)|リンク(AIDB))
PAT(リンク(AIDA)|リンク(AIDB))
MakePAT
AIDA
AIDB
Enabler of AIDA
Enabler of AIDB
有効期限情報
移転制御情報
ユーザA
AIDB
Enabler of AIDB

装置構成(7)

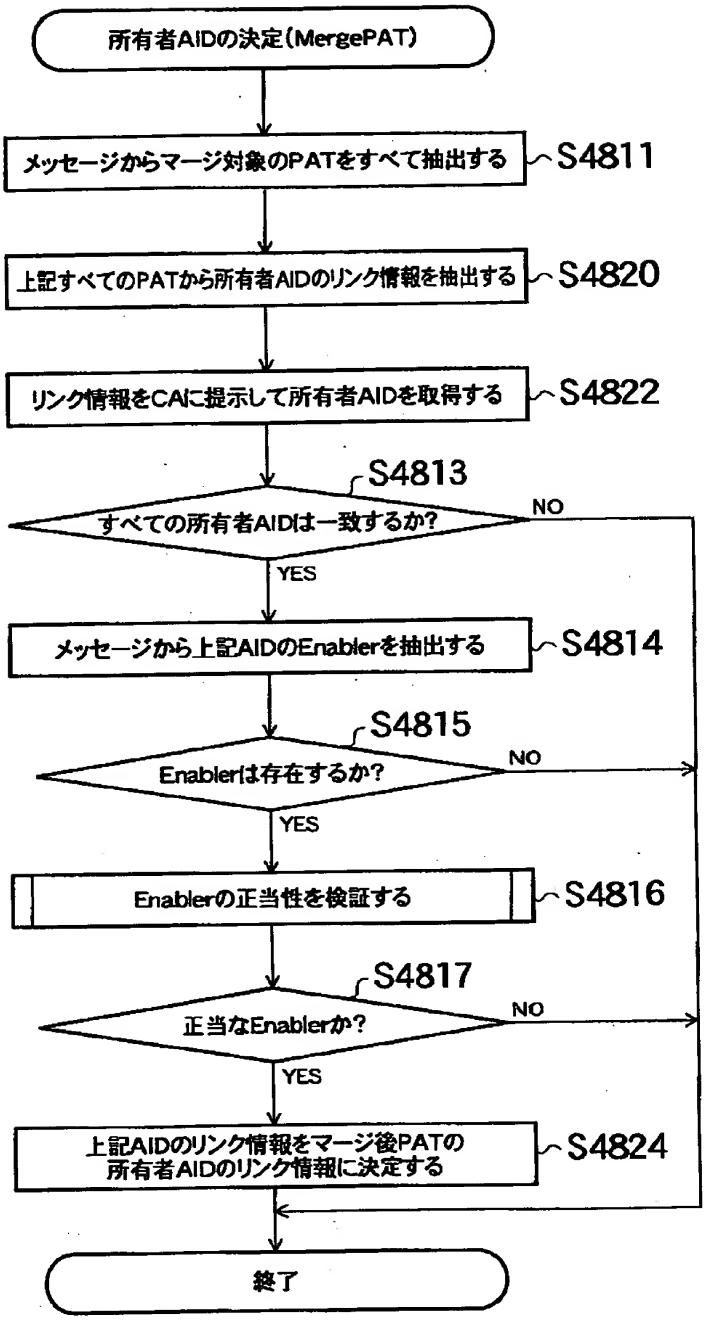
【図９０】


AIDリストの生成
(MakePAT.MergePAT.SplitPAT.TransPAT)
バッファ長を決定する
S4611
バッファを生成する
S4612
所有者AIDのリンク情報を上記バッファの空き領域にコピーする
S4617
会員AIDのリンク情報を上記結果の空き領域にコピーする
S4618
S4615
次の会員AIDは存在するか?
YES
NO
終了

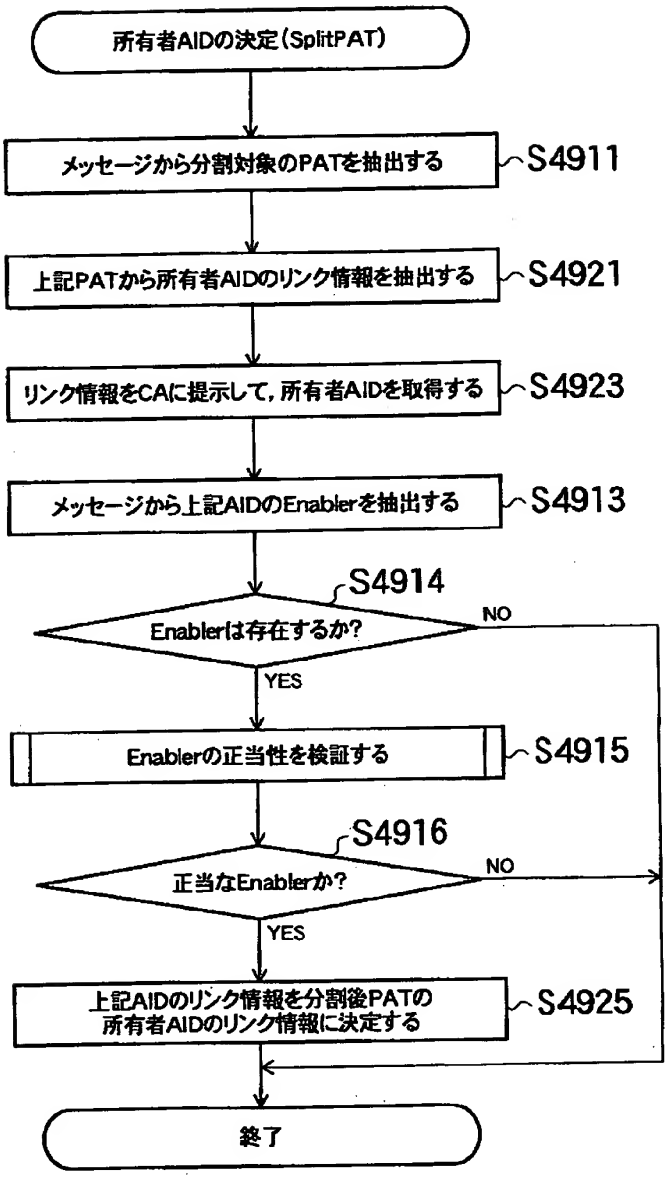
【図９１】


所有者AIDの決定(MakePAT)
メッセージから所有者AIDにしたいAIDを抽出する
S4711
S4712
上記AIDは存在するか?
NO
YES
メッセージから上記AIDのEnablerを抽出する
S4713
S4714
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S4715
S4716
正当なEnablerか?
NO
YES
上記AIDのリンク情報を新規生成PATの
所有者AIDのリンク情報に決定する
S4718
終了

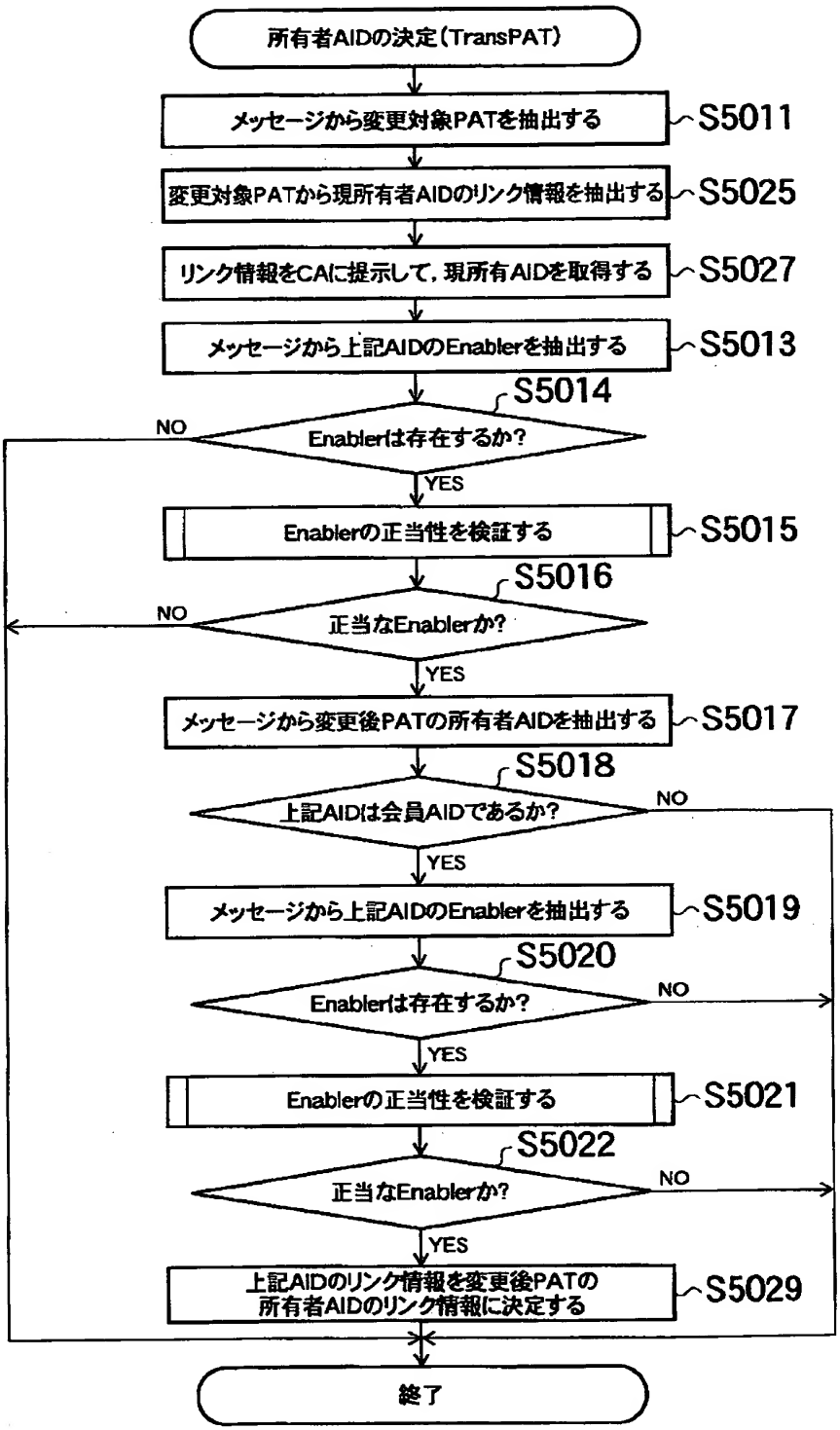
【図９２】


所有者AIDの決定(MergePAT)
メッセージからマージ対象のPATをすべて抽出する
S4811
上記すべてのPATから所有者AIDのリンク情報を抽出する
S4820
リンク情報をCAに提示して所有者AIDを取得する
S4822
S4813
すべての所有者AIDは一致するか?
NO
YES
メッセージから上記AIDのEnablerを抽出する
S4814
S4815
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S4816
S4817
正当なEnablerか?
NO
YES
上記AIDのリンク情報をマージ後PATの
所有者AIDのリンク情報に決定する
S4824
終了

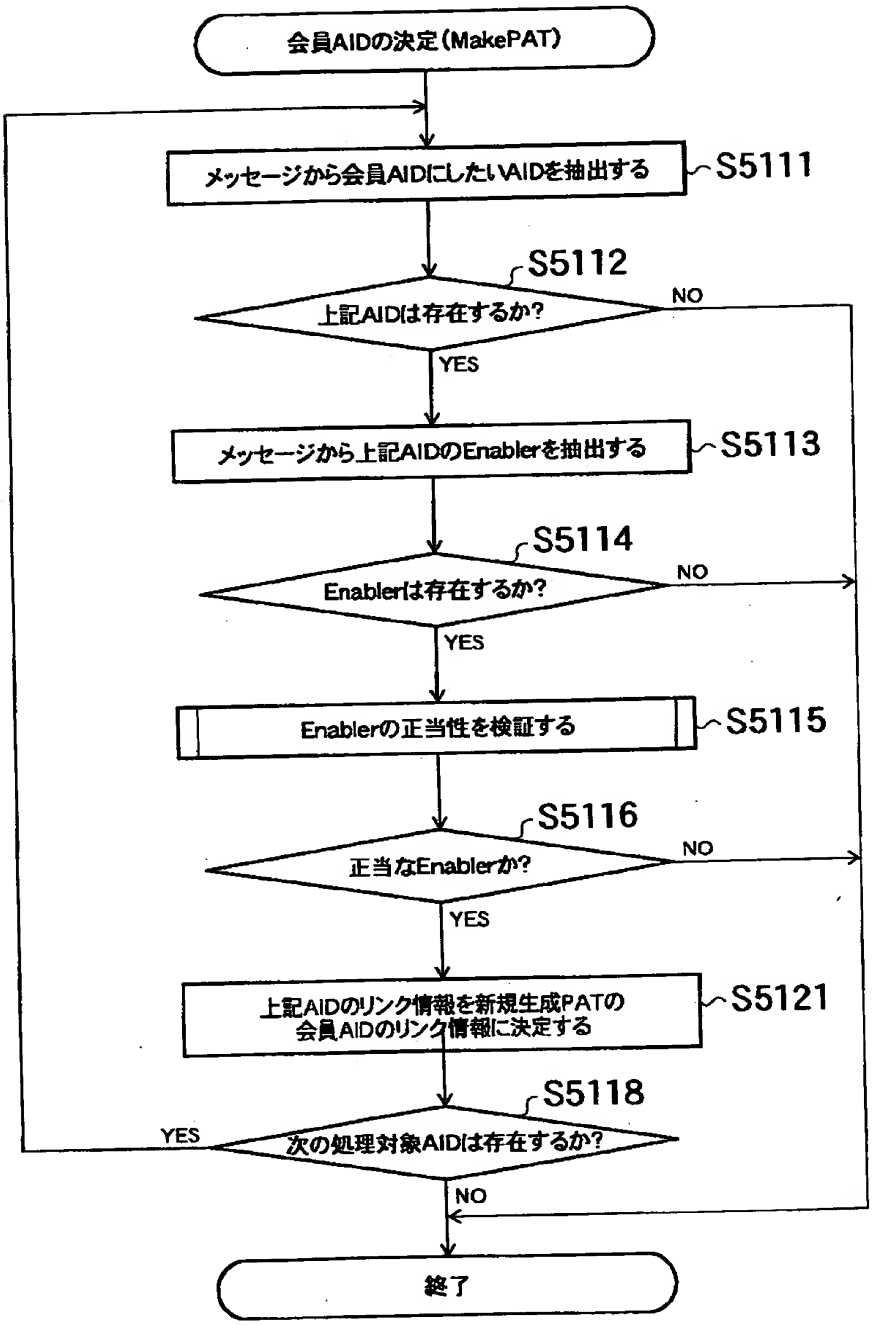
【図９３】


所有者AIDの決定(SplitPAT)
メッセージから分割対象のPATを抽出する
S4911
上記PATから所有者AIDのリンク情報を抽出する
S4921
リンク情報をCAに提示して，所有者AIDを取得する
S4923
メッセージから上記AIDのEnablerを抽出する
S4913
S4914
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S4915
S4916
正当なEnablerか?
NO
YES
上記AIDのリンク情報を分割後PATの
所有者AIDのリンク情報に決定する
S4925
終了

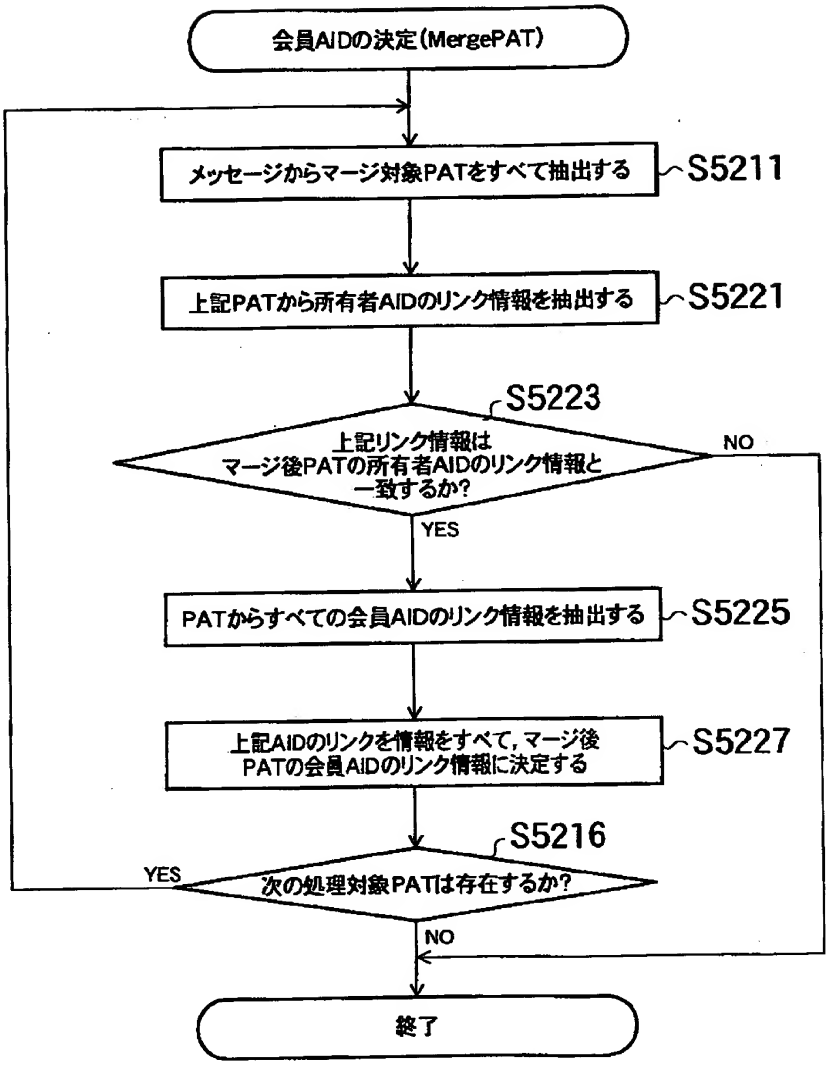
【図９４】


所有者AIDの決定(TransPAT)
メッセージから変更対象PATを抽出する
S5011
変更対象PATから現所有者AIDのリンク情報を抽出する
S5025
リンク情報をCAに提示して，現所有AIDを取得する
S5027
メッセージから上記AIDのEnablerを抽出する
S5013
S5014
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S5015
S5016
正当なEnablerか?
NO
YES
メッセージから変更後PATの所有者AIDを抽出する
S5017
S5018
上記AIDは会員AIDであるか?
NO
YES
メッセージから上記AIDのEnablerを抽出する
S5019
S5020
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S5021
S5022
正当なEnablerか?
NO
YES
上記AIDのリンク情報を変更後PATの
所有者AIDのリンク情報に決定する
S5029
終了

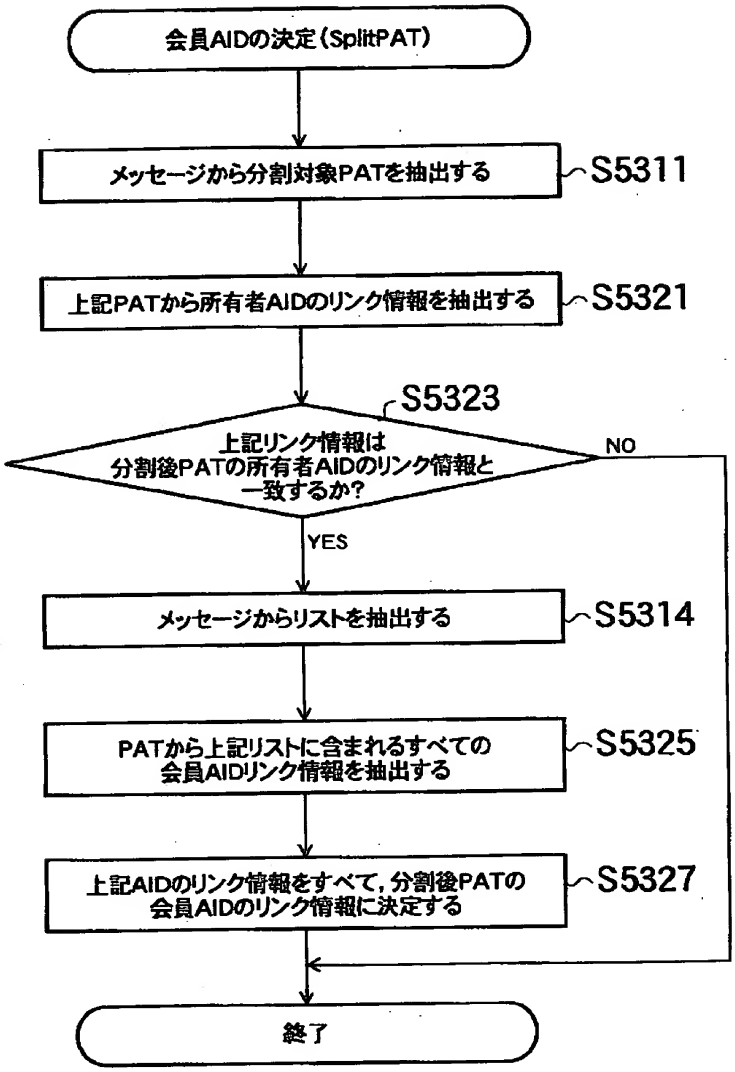
【図９５】


会員AIDの決定(MakePAT)
メッセージから会員AIDにしたいAIDを抽出する
S5111
S5112
上記AIDは存在するか?
NO
YES
メッセージから上記AIDのEnablerを抽出する
S5113
S5114
Enablerは存在するか?
NO
YES
Enablerの正当性を検証する
S5115
S5116
正当なEnablerか?
NO
YES
上記AIDのリンク情報を新規生成PATの
会員AIDのリンク情報に決定する
S5121
S5118
YES
次の処理対象AIDは存在するか?
NO
終了

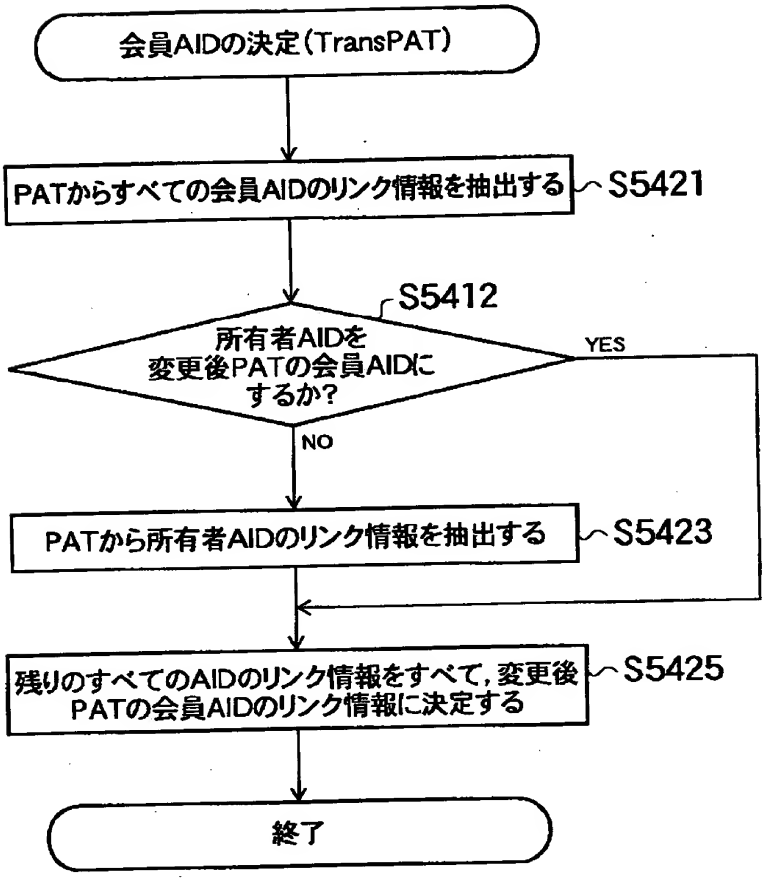
【図９６】


会員AIDの決定(MergePAT)
メッセージからマージ対象PATをすべて抽出する
S5211
上記PATから所有者AIDのリンク情報を抽出する
S5221
S5223
上記リンク情報は
マージ後PATの所有者AIDのリンク情報と
一致するか?
NO
YES
PATからすべての会員AIDのリンク情報を抽出する
S5225
上記AIDのリンクを情報をすべて,マージ後
PATの会員AIDのリンク情報に決定する
S5227
S5216
YES
次の処理対象PATは存在するか?
NO
終了

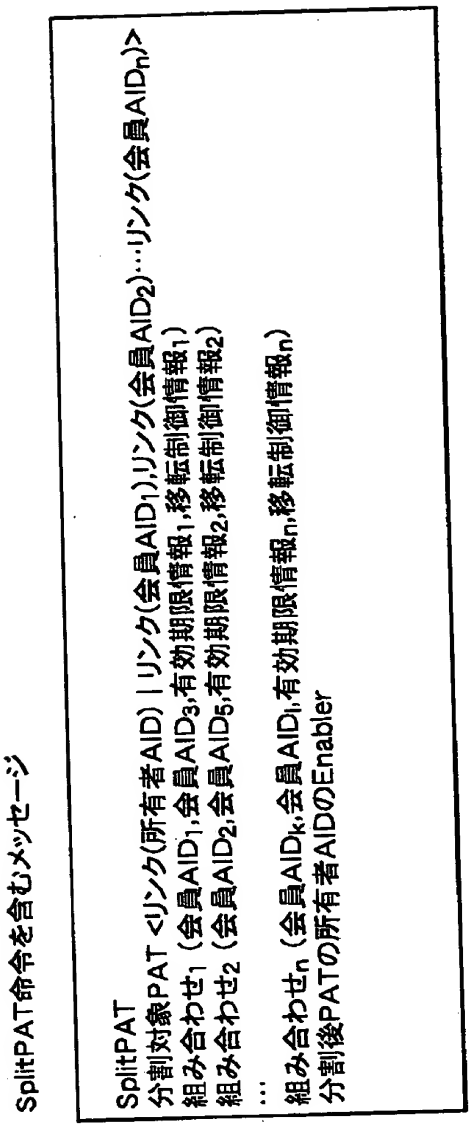
【図９７】


会員AIDの決定(SplitPAT)
メッセージから分割対象PATを抽出する
S5311
上記PATから所有者AIDのリンク情報を抽出する
S5321
S5323
上記リンク情報は
分割後PATの所有者AIDのリンク情報と
一致するか?
NO
YES
メッセージからリストを抽出する
S5314
PATから上記リストに含まれるすべての
会員AIDリンク情報を抽出する
S5325
上記AIDのリンク情報をすべて,分割後PATの
会員AIDのリンク情報に決定する
S5327
終了

【図９８】


会員AIDの決定(TransPAT)
PATからすべての会員AIDのリンク情報を抽出する
S5421
S5412
所有者AIDを
変更後PATの会員AIDに
するか?
YES
NO
PATから所有者AIDのリンク情報を抽出する
S5423
残りのすべてのAIDのリンク情報をすべて,変更後
PATの会員AIDのリンク情報に決定する
S5425
終了

【図９９】


SplitPAT命令を含むメッセージ
SplitPAT
分割対象PAT <リンク(所有者AID)｜リンク(会員AID1),リンク(会員AID2)…リンク(会員AIDn)>
組み合わせ1（会員AID1,会員AID3,有効期限情報1,移転制御情報1）
組み合わせ2（会員AID2,会員AID5,有効期限情報2,移転制御情報2）
…
組み合わせn（会員AIDk,会員AIDl,有効期限情報n,移転制御情報n）
分割後PATの所有者AIDのEnabler

【図１００】

TransPAT命令を含むメッセージ

TransPAT
所有権変更対象PAT <リンク(所有者AID)｜リンク(会員AID_1),リンク(会員AID_2),…リンク(会員AID_n)>
所有者AIDのEnabler
所有権変更後PATの所有者AID　左記AIDのEnabler
有効期限情報
移転制御情報

【図１０１】

MergePAT命令を含むメッセージ

MergePAT
マージ対象PAT <リンク(所有者AID) | リンク(会員AID_{11}),リンク(会員AID_{12})…リンク(会員AID_{1n})>
マージ対象PAT <リンク(所有者AID) | リンク(会員AID_{21}),リンク(会員AID_{22})…リンク(会員AID_{2n})>
…
マージ対象PAT <リンク(所有者AID) | リンク(会員AID_{m1}),リンク(会員AID_{m2})…リンク(会員AID_{mn})>
マージ後PATの所有者AIDのEnabler
有効期限情報
移転制御情報

【書類名】　　要約書

【要約】

【課題】　匿名性とセキュリティを確保すべく着信者の匿名性を保持しつつ発信者からの通信の接続を可能とする接続制御方法および通信網と接続制御プログラムおよびデータ構造を記録した記録媒体を提供する。

【解決手段】　ユーザに役割識別子を付与し、役割識別子とユーザに関する情報を閲覧可能に保持し、発信者は着信者を役割識別子で指定し、この指定に基づき発信者に発信者フラグ、移転制御フラグ、有効期限を含む個別化アクセスチケットを発行し、役割識別子と個別化アクセスチケットを用いて個別化アクセスチケットが有効期限内で正当であり、発信者役割識別子が個別化アクセスチケットに含まれ、着信者役割識別子が個別化アクセスチケットに含まれていることを検証し、検証結果がすべて正しい場合に発信者からの接続要求を通信網の物理的な接続制御方式に変換する接続制御を行う。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000004226
【住所又は居所】　東京都新宿区西新宿三丁目１９番２号
【氏名又は名称】　日本電信電話株式会社
【代理人】　申請人
【識別番号】　100083806
【住所又は居所】　東京都港区虎ノ門１丁目２番３号　虎ノ門第一ビル９階　三好内外国特許事務所
【氏名又は名称】　三好　秀和
【選任した代理人】
【識別番号】　100068342
【住所又は居所】　東京都港区虎ノ門１丁目２番３号　虎ノ門第一ビル９階　三好内外国特許事務所
【氏名又は名称】　三好　保男

出 願 人 履 歴 情 報

識別番号　〔０００００４２２６〕

１．変更年月日　１９９５年　９月２１日
［変更理由］　住所変更
住　所　東京都新宿区西新宿三丁目１９番２号
氏　名　日本電信電話株式会社